

Report to the Court

Failure to Preserve Data

On January 22nd 2021, Mr. Davis, Attorney for the Plaintiffs in this matter, filed an Amended Motion for Temporary Restraining Order. I obtained a copy of the Motion and contacted Mr. Davis regarding a few of my concerns about certain points within the Motion that I believed needed clarification because they would not be inherently clear to any person lacking significant experience in data and/or networking systems. In preparing this report, I reviewed all of the openly available marketing and operational manuals for the electronic voting machines used by the states, and counties mentioned in this report and supporting documents. Additionally, I reviewed the referenced, and mentioned laws and conduct of states referenced in a Stanford-MIT report, which I use to illustrate components of concern to inform the Court. Further, I utilized my network of forensic investigators, ethical hackers, and network engineers to obtain easily discernable and understandable content from which the Court would reasonably be capable of understanding the complexities of technology mentioned in the report, and supplementals attached to this report.

In certain areas I relied on my own personal experience in process management, combined with knowledge of governmental financial regulations, and years of experience operating highly technical communications and network operating companies. Finally, regarding deeper global financial issues, I consulted with multiple peers who would be considered experts in their field and who operate companies within the global financial sector with the specific focus on current “market maker” movements which would lead to a shift in reserve currency status.

As I stated to Mr. Davis my concerns arise from a strict reading of the language provided in the Civil Rights Act of 1960, Section 301. Further, on a process management level I have extreme concerns for glaring failures of state election officials to comply with very specific requirements of the Help American Vote Act of 2002’s section 303. Regarding HAVA, I have a procedural concern, as well as a civil rights records concern, which arises from the 1960 Civil Rights Act.

When I spoke with Mr. Davis, I addressed a concern with him regarding **Section 301 of the 1960 Civil Rights Act** which states “*Every officer of Election shall retain and preserve*” then stipulates the type of elections to include all federal offices. **Section 301** then clearly states “*all records and papers which come into his possession.*” The act clearly stipulates all records and papers which comes into the possession of “*every officer of election*” and then mandates the retention of, and preservation of, said “*all records*” for 22 months. 52 U.S.C. § 20701

“The Process Concern”

Section 303 of the Help America Vote Act is particularly of concern in the 2020 federal election due to the sheer number of first-time federal mail in ballot voters. In **Exhibit 1**¹ attached hereto, the authors did an excellent job of compiling information regarding the voting processes, mail in ballot procedures, and processes used by the “swing” states of Arizona, Florida, Michigan, North Carolina, Pennsylvania, and Wisconsin. The information is provided by the **Stanford-MIT Healthy Elections Project**² and upon further review the facts presented within the report are correct relevant to this Report. The Stanford-MIT report shows the significant rise in mail in ballots in the 2020 federal election with the largest increase being 625% increase in federal mail in and/or absentee ballots compared to 2016 within the State of Wisconsin. Due to this, it is reasonable to conclude more than one million ballots in the state were cast by voters who voted for the first time by mail in a federal election. I must bring to the Court’s attention according to **Section 209 of the Help America Vote Act** “*the commission*” meaning the EAC, does not have “*any authority to issue any rule, promulgate any regulation, or take any other action*” upon a state to alter the Act, its requirements or impose any duty upon a state, or grant a relief or special exception to a state, including modifying “minimum requirements” of **Section 304**.

¹ “From Tabulation to Certification: How Battleground States Count the Vote” Authors Jennifer Friedmann, J.D. ’22; Toni Friedman, M.A in International Policy ’21; Jesus Lazarus, J.D. ’22, Albert Park, J.D. ’22, Alex Stout, B.A. ’22; Sydney Frankenber, M.A. in International Policy ’21; Andriana Stephan, M.A. in International Policy ’21; Alez Zaheer, M.A. ’21 Healthy Elections. Org ; October 30th, 2020. (Exhibit 1)

² The project is led by [Professor Nathaniel Persily](#), James B. McClatchy Professor Law at Stanford and former Senior Research Director of the Presidential Commission on Election Administration, and [Charles Stewart III](#), Kenan Sahin Distinguished Professor of Political Science at MIT, Director of the [MIT Election Data and Science Lab](#), and Co-Director of the [Caltech/MIT Voting Technology Project](#).

My first process concern is directly tied to HAVA Section 303 (b),³ which mandates a DUTY ON THE STATE regarding “first time voters” registered by and/or voting by mail to obtain data which determines if the “person” had “previously voted in an election for federal office.” This duty upon the state creates a PAPER document trail that in many instances MUST accompany the ballot and, pursuant to the Civil Rights Act of 1960, Sec. 301, be maintained for 22 months, with the original ballot. A careful but quick review of the Stanford-MIT Report will show this Honorable Court that all of the swing states separate ballots from “papers” and “envelopes” in the pre-tabulation process. Further, there is NO mention in any state procedure regarding the verification of the PAPER requirement generated in HAVA’s Section 303.

The second “process” concern is directly tied to the RETENTION of ALL papers which come into the possession of “election officials.” A review of the procedures in all swing states within the reports quickly shows the separation of records / papers, and items that come into the possession of election officials. It would seem even on the most minor level, disposal of the envelopes themselves would violate **Sec. 301 of the Civil Rights Act**. But of most concern is the discarding of ANY paper from ANY voter who submitted the required paperwork as stipulated in HAVA’s section 303. It is clear that most of the states, according to the Stanford-MIT report, under state law, use only the signature verification requirement, which is insufficient to vote for first time by mail or registered by mail, mail in or absentee voters pertaining to the federal election. Logically, due to Congress’s use of their Constitutional authority⁴ to place regulations, as it did in the **Help America Vote Act**, these violations of federal law must also be considered violations of the Constitution pertaining to the conduct of a federal election, especially for the House of Representatives (the states are also required to follow HAVA for Senate elections because they received federal funds in exchange for the agreement to follow HAVA).

These are not the only “process concerns” that I have, but these are the easiest of the process concerns to address. I must state to the Court that the vast majority of the states saw a significant rise in mail in ballots, none of them complied with the aforementioned process issues listed.

³ Help America Vote Act Sec. 303 (b)(1)(B)(i)

⁴ U.S. Constitution, Article I, Section 4.

Additionally, according to the **National Conference of State Legislatures**⁵ the states of Colorado, Oregon, and Washington conduct ALL of their elections by mail, and as many as “22 states have certain provisions that allow certain elections to be conducted entirely by mail.” Of concern here is that cases collectively known as the “Trump vs Biden” election challenges moving to the Supreme Court ALL fail to address or recognize the states of California and Nevada conducted their entire elections by mail out / mail in ballot in 2020, and both states failed to meet the requirements of HAVA as shown above and here within.

Logically, even IF it were possible to make “finding” in these elections’ cases, neither Mr. Trump nor Mr. Biden could obtain a majority in the electoral college due to the failures to comply with federal law, and the nullity issue pertaining to the House of Representatives issues arising from the Plaintiff’s claims, and direct legal challenges for civil rights / constitutional election challenge

Clear Civil Rights records retention violations.

Upon review of ALL of the State’s processes and machine voting systems something became glaringly clear, each state relied 100 percent on the tabulation machine being accurate, and NONE of the states conducted a “manual recount” unless the election results were within a less than 1% margin between candidates for office. This places a HUGE concern on several levels. First of which pertains to Attorney General Barr’s December 1st, 2021 comment in which he stated “there was no widespread evidence of election fraud.”⁶ Mr. Barr’s commentary was frivolous and illegitimate, as no voting machine was seized and forensically audited. Further, no state conducted a manual recount⁷ of the entire ballot pool, and those that did recount used the tabulation machines previously used. In short, there was NO forensic audit of the ballots themselves, only the “paper” receipts created by the voting machines! This “system” of “audit” would not meet any requirement of the federal government’s own regulations pertaining to the Securities and Exchange Commissions purview.

⁵ <https://www.ncsl.org/research/elections-and-campaigns/all-mail-elections635457869.aspx> (Exhibit 2)

⁶ <https://apnews.com/article/barr-no-widespread-election-fraud-b1f1488796c9a98c4b1a9061a6c7f49d> (Exhibit 3)

⁷ Meaning “BY HAND”

Additionally, according to the **National Conference of State Legislatures**⁵ the states of Colorado, Oregon, and Washington conduct ALL of their elections by mail, and as many as “22 states have certain provisions that allow certain elections to be conducted entirely by mail.” Of concern here is that cases collectively known as the “Trump vs Biden” election challenges moving to the Supreme Court ALL fail to address or recognize the states of California and Nevada conducted their entire elections by mail out / mail in ballot in 2020, and both states failed to meet the requirements of HAVA as shown above and here within.

Logically, even IF it were possible to make “finding” in these elections’ cases, neither Mr. Trump nor Mr. Biden could obtain a majority in the electoral college due to the failures to comply with federal law, and the nullity issue pertaining to the House of Representatives issues arising from the Plaintiff’s claims, and direct legal challenges for civil rights / constitutional election challenge

Clear Civil Rights records retention violations.

Upon review of ALL of the State’s processes and machine voting systems something became glaringly clear, each state relied 100 percent on the tabulation machine being accurate, and NONE of the states conducted a “manual recount” unless the election results were within a less than 1% margin between candidates for office. This places a HUGE concern on several levels. First of which pertains to Attorney General Barr’s December 1st, 2021 comment in which he stated “there was no widespread evidence of election fraud.”⁶ Mr. Barr’s commentary was frivolous and illegitimate, as no voting machine was seized and forensically audited. Further, no state conducted a manual recount⁷ of the entire ballot pool, and those that did recount used the tabulation machines previously used. In short, there was NO forensic audit of the ballots themselves, only the “paper” receipts created by the voting machines! This “system” of “audit” would not meet any requirement of the federal government’s own regulations pertaining to the Securities and Exchange Commissions purview.

⁵ <https://www.ncsl.org/research/elections-and-campaigns/all-mail-elections635457869.aspx> (Exhibit 2)

⁶ <https://apnews.com/article/barr-no-widespread-election-fraud-b1f1488796c9a98c4b1a9061a6c7f49d> (Exhibit 3)

⁷ Meaning “BY HAND”

Indeed, the uniform standard for audit within the United States is known as Generally Accepted Accounting Practices (GAAP) which within a “validation” process require a manual reevaluation of each element of an audit, not a cursory review of sub-tabulated columns! How can any party believe the economic and geo-political stability of the nation, and in many cases the world be less acceptable than a party balancing a check book? It’s a preposterous notion. In short, the “no fraud” statement was made by a review of printed audit forms created by the tabulation system itself, not by a manual audit conducted by agents, or scientists. This itself is a concern, as this “no evidence” frivolity has been over-populated in the media *in extremis*. It is simply not factually correct to say there is no evidence of fraud when there has never been a venue that reviewed “evidence” and there was no audit from which to conclude “no fraud”. Now in this matter, we are not concerned about the outcome of Trump/Biden, but we are concerned about the retention of actual records, an audit of facts, and the legitimacy of conduct by those who conducted the first all-electronic federal election.

Mr. Trump’s legal team has presented a theory that “machines flipped” or “changed votes” in the Presidential election. Yet NO machine was seized and forensically examined by any law enforcement agency. Further, no forensic exam was conducted by ANY legal team, or team’s experts on the hardware itself. As shown in Exhibit 4⁸ attached here to, it is possible using a variety of techniques to embed hidden software / programs / application into a machines hardware which are undetectable without forensic review. Also, as shown in Exhibit 5⁹ there are a variety of “anti-forensic” techniques that hackers / bad actors can use to conceal digital activities. As stated in the article *“Anti-forensic techniques can make a computer investigator’s life difficult. From committing fraud in an organization to stealing crucial data, cybercriminals can perform a wide range of nefarious activities. In some cases, these perpetrators try to cover their tracks by deleting browser history, cache memory, and even cookies.”* This “cover their tracks” comment is most troubling as EACH company which sells election tabulation equipment details a “wipe” of the tabulation equipment. In Georgia, the state has repeatedly been “blasted” by judges¹⁰ and

⁸ Information Hiding and Detection – Department of Computer Science and Engineering, Mississippi State University. (Exhibit 4)

⁹ <https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/> (Exhibit 5)

¹⁰ <https://www.yourbasin.com/news/national/judge-blasts-georgia-officials-handling-of-election-system/> (Exhibit 6)

others for “wiping” election equipment and in 2020 Georgia once again “wiped” their election equipment in preparation for a “run-off” election despite two lawsuits being filed by prominent lawyers regarding election fraud.¹¹

It is clear, in 1960 the Congress without forward vision of the emerging technologies could not envision the word “records” to include electronic records, random access memory, phantom memory, or the literal 100’s of ways a cybercriminal could embed information within a piece of computer hardware. However, Congress was VERY CLEAR on their intent to secure, preserve, and maintain ALL RECORDS. Obviously, anything that preserves “data” would meet the ordinary definition of a “record.”¹² Since the “election machines” are still in the possession of state election officials, but the states “wiped” the machines, this failure to maintain these electronic records held within the machines themselves for 22 months is in itself a civil rights violation for the exact reason the Congress mandated the requirement to hold records. Which was to determine IF crimes / violations of civil rights had occurred.

Mr. Davis’s questions.

Mr. Davis provided six questions to me. I believe these questions may assist the Court in obtaining clarity to the Plaintiff’s complaint, but I must clearly state the issue before the Court has significant “public interest” merit, and accordingly I encourage the Court to grant the Plaintiff’s TRO, so forensic teams from a lawful federal government can instigate a criminal investigation into acts of conspiracy. Mr. Davis’s Questions to me and my direct answers are as follows:

1. How is “data hiding” related to Plaintiffs' causes of action in this lawsuit?

It is clear the Congress mandated the “preservation” of records relating to elections as a method not only to assure the outcome of an election but also to determine if any unlawful conduct had occurred within the election itself. Specifically, the Congress was concerned if some “bad actor” could manipulate the vote, inhibit a person’s liberty interests, disenfranchise voters of color, and conduct criminal acts, including acts of fraud. While this is not directly stated in the Civil Rights

¹¹ <https://247sports.com/college/usc/board/59419/Contents/-judge-allows-ga-to-reset-wipe-dominion-voting-machines-data-155673790/> (Exhibit 7)

¹² Civil Rights Act 1960 Sec 301-304 highlighted (Exhibit 8)

Act of 1960 in one sentence, This intent is clear from a combination of statement, direction, and requirements, not to mention the historical context of HAVA in the wake of the Bush v. Gore election debacle. **It is self-evident that every citizen has a right to a “transparent” election process, and** the federal government has a duty to ensure “*a republican form of government.*”¹³ The Defendants conduct to prohibit the audit of election hardware prior to “wiping” and “warehousing” is a clear destruction of records in the possession of election officials, which is a clear violation of **Sec. 301 of the Civil Rights Act**, which has penalties described for “each” person who engaged in such conduct in **Sec. 302, 303, and 304.**

2. What is the relevance of the data hiding techniques?

Data hiding techniques destabilize results and erode voter confidence in the electoral process. This, coupled with the states’ procedural “failures” to comply with HAVA’s multiple certification processes, and the failures to obtain, retain, or preserve first-time mail in voter information makes it almost impossible to certify all outcomes of all federal offices as anything other than a fraudulent act. Without a clear audit of hardware or software and a hand recount of ballots, there is no such thing as an “audited” election. Further, a forensic examination will review the conduct of actors in the election process. Pertaining to relevance, how secure and honest are the machines? And factual are the tabulated results? In my opinion it’s highly relevant overall.

3. Do you have grounds to believe there is hidden data on the machines?

Absolutely. No person outside of the software companies have been allowed to review the “proprietary software” of the election machine companies. As reported in Politico on Nov. 3rd 2020, “*Most voting technology used throughout the U.S. is covered by intellectual property law. That means the touch-screen you might have tapped on to vote could be patented. The software used to process your vote could be copyrighted. Before you even got to the voting booth, your ballot was likely designed on copyrighted software.*”¹⁴ By the very definition, this lack of review makes all “data” on the machines “hidden.” Also, by law, the states have to maintain this data / record, including the software itself for 22 months. But, in several states, and counties once the

¹³ U.S.Constitution, Article IV, Section 4.

¹⁴ Exhibit 9 (Politico – 1/25/21)

“contract” for an election is over the machines are removed, and so goes the “records” of the election in the “all records” category.

4. If the data is hidden how would you discover it?

Pertaining to nefarious data, or “botware,” which could be used to flip votes, fraudulently tabulate ballots, or to “stuff ballot boxes,” there are more than 100 forensic techniques to find malware or fraudulent conduct within the drive space. There are additional hardware monitoring techniques that reveal “hidden” processes that are not viewable by a software review, code review,¹⁵ or hard drive analysis based upon system loads, electrical usage, and machine systems operations. There are also methods to mirror systems on to “clean” hardware which reveals nefarious systems and operations. My recommendation is to ask a team of professionals, such as Mr. Cain,¹⁶ to review the software systems, then conduct a hardware system load analysis to find any malware systems mechanically.

5. Why should the judge risk ordering an audit of the machines? Won't it ruin his career if he orders an audit that turns up nothing?

If we are to remain a nation of laws, then the Judge in this matter MUST grant the TRO in this matter. As far as ordering a forensic audit of machines, I am not aware of a SINGLE machine that was used in the 2020 election that has not been wiped post-election due to “decommissioning” and “warehousing” or “run-off election” procedures. However, a review of the operating systems which are, by nature, hidden from review of the public and election officials under an absurd “copyright” argument will reveal any conduct or systems / activities alleged in any of the hundreds of election fraud lawsuits that are moving towards the Supreme Court.¹⁷ At this point, the Judge’s act would seem to be nothing more than a “friend of the court” activity, which would assist the Supreme Court in reviewing these cases.

¹⁵ Introduction to Hiding and Finding Data on Linux (GAIC Certification Series) (Exhibit 10)

¹⁶ Mr. Cain submitted a report as part of the Plaintiff’s Complaint illustrating multiple calibration/ certification issues, as well as stated his expertise in forensic / compliance issues. (Exhibit 2 to Plaintiffs’ Original Complaint).

¹⁷

**6. Can you offer the Court anything beyond mere speculation that there is hidden data on the machines, and that you could find it?
How likely is it? Over 50% chance? Less than 50% chance?**

Based upon my 20 plus years of experience in the networking / communications / internet / technology space, I can concluded with near certainty that “hidden data” would be revealed¹⁸. I am more than certain that a team of forensic auditors will find a series of anomalies, errors in code, and malware within more than just Dominion Voting’s systems. As most of the companies use a common foot print and operating system readily available in the retail sector, it would be irrational to assume any of the systems are immune from, or secure from malfeasant conduct, wether by the companies themselves or cybercriminals who obtained access at various stages of the pre-election / election / post-election process. No matter what the outcome of the audit, the records on the machines themselves are mandated to be preserved, and it is very apparent a large portion of the “records” held in the possession of election officials during the election process do not remain in possession or secured as required in the Civil Rights Act of 1960.

Conclusion

The public interest issue that emanates from the Plaintiff’s legal action is graphically multiplied when viewed against the post-election conduct of the Defendants who are beneficiaries of the unlawful election. As a Veteran, I am shocked by the repeated unconstitutional conduct of the 117th House of Representatives and many Senators, who obtained office by unconstitutional, and unlawful processes. I am bewildered by the brazen arrogance in the Senate scheduling the impeachment trial of a now-private citizen of the United States without lawful right. I am deeply concerned of the calculated injuries inflicted on our nation’s financial mechanisms which could cause a geo-political shift and stimulate the emergence of a new global reserve currency. I foresee in the not-so-distant future the globe will not speak of the “dollar” as a unit of currency, but will instead reference the “yuan.” As stated in the Global Risk Report, once the world realizes the

¹⁸ Based upon the knowledge that no third party has been afforded the ability to review any portion of the EVM’s operating systems, or other components of systems integration software. Due to this, by very definition, all of the software / hardware configuration and sub programming is ‘hidden’ and contains ‘hidden data’.

Congress and President are not legitimately seated into office, this country will no longer be a safe haven, because it will no longer be known as a nation that abides by “the rule of law”.

Respectfully Submitted

/s/ John S. Vanderbol III

John S. Vanderbol III

Exhibit 1.

From Tabulation to Certification: How Battleground States Count the Vote

October 30, 2020

When voters drop their absentee ballots in a mailbox, or feed their completed ballot into a ballot box at a polling place, their act of voting is over. But for election officials, the process has a long way to go. Receiving a voter's ballot is the first in a long list of tasks specific to the goal of seeing that all ballots—whether they are cast in person or through the mail—are accurately processed, counted, reported, and certified.

Key swing states take different approaches to these tasks. In Michigan, Pennsylvania, and Wisconsin, state law prevents election officials from processing or counting votes until Election Day. By contrast, Florida, North Carolina, and Arizona explicitly permit officials to start processing ballots before Election Day, with Florida and Arizona also permitting officials to begin counting ballots before Election Day. In these swing states, like all others, election officials have prepared to accommodate the anticipated surge in the number of ballots cast by mail while complying with laws that were written in anticipation of much lower numbers. Some states such as Florida have anticipated the influx of mail-in ballots by proactively taking measures to permit counting even earlier than what is statutorily required. In addition to states needing to prepare themselves to accommodate the surge, voters must also prepare themselves for how the results will be reported to the public and later formally certified.

This report breaks down the processes for counting the vote in six swing states. It explains how and when these battleground states count ballots and report results, starting with the processing of mail-in ballots and following through the tabulation of results, election night reporting, and final certification of election results.

Authors: Jennifer Friedmann, J.D. '22; Toni Friedman, M.A. in International Policy '21; Jesse Lazarus, J.D. '22; Albert Park, J.D. '22; Alex Stout, B.A. '22; Christopher Wan, J.D./M.B.A. '23; Chase Small, B.A. '22; Sydney Frankenberg, M.A. in International Policy '21; Adriana Stephan, M.A. in International Policy '21; Alez Zaheer, M.A. International Policy '21

Table of Contents

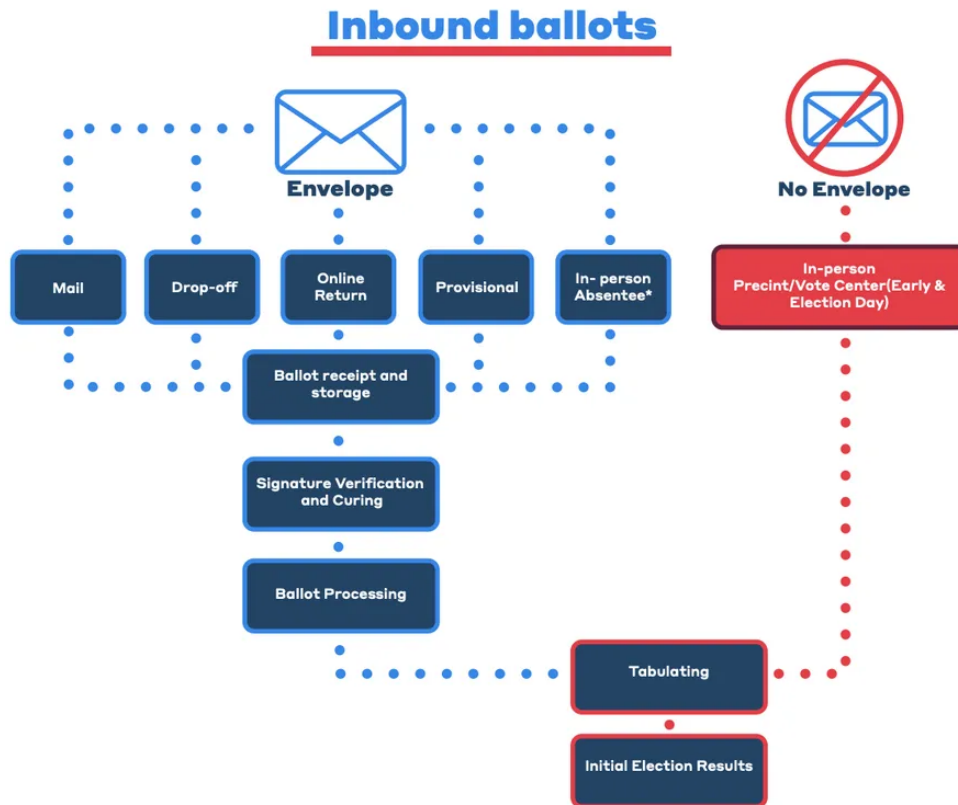
| | |
|----------------------------|-----------|
| Introduction | 3 |
| Arizona | 6 |
| Processing Mail-In Ballots | 6 |
| Tabulating the Vote | 7 |
| Reporting the Vote | 9 |
| Certifying the Vote | 9 |
| Florida | 10 |
| Processing Mail-In Ballots | 10 |
| Tabulating the Vote | 11 |
| Reporting the Vote | 12 |
| Certifying the Vote | 13 |
| Michigan | 13 |
| Processing Mail-In Ballots | 14 |
| Tabulating the Vote | 15 |
| Reporting the Vote | 16 |
| Certifying the Vote | 16 |
| North Carolina | 17 |
| Processing Mail-In Ballots | 18 |
| Tabulating the Vote | 21 |
| Reporting the Vote | 22 |
| Certifying the Vote | 22 |
| Pennsylvania | 24 |
| Processing Mail-In Ballots | 25 |
| Tabulating the Vote | 27 |
| Reporting the Vote | 28 |
| Certifying the Vote | 28 |
| Wisconsin | 29 |
| Processing Mail-In Ballots | 30 |
| Tabulating the Vote | 32 |
| Reporting the Vote | 34 |
| Certifying the Vote | 35 |
| Conclusion | 35 |
| Appendix | 36 |

Introduction

This memo covers four stages of counting the vote: processing mail ballots, tabulating results, reporting results, and certifying the vote. These processes vary widely by state, both in terms of statutory requirements and administration. In each of the six swing states described below, we examine when and how ballots are counted, who does the counting and reporting, and how much discretion states give to local officials. We order this examination in four steps (with credit to research by the [Bipartisan Policy Center](#) for these overviews):

Processing Mail-In Ballots: Processing mail-in ballots is also called [pre-processing](#) ballots. Mail-in ballots, or any other ballot cast in an envelope, such as in-person absentee ballots or some provisional ballots, must be handled differently than ballots cast by an identity-verified voter in a polling place. When a voter is not present in person, an election administrator must check the voter's identification and eligibility to vote. States often look for and verify voters' signatures certifying that they are indeed the voters whose names appear on the ballot; some states require a witness to sign as well. Once the voter's identity is verified, the envelope is opened and the ballot is separated from any identifying information. For states that use secrecy sleeves, those interior envelopes are also removed and the ballots are flattened and prepared for tabulation, either at a precinct or a central tabulation facility.

The [Bipartisan Policy Center](#) compares the process for mail-in ballots (with an envelope) versus in-person ballots in this graphic:



The timing of mail-in ballot processing varies across the country. Some states begin processing ballots weeks in advance, while others are only allowed to begin on Election Day. States that begin early may have more results counted by election night. In the six swing states analyzed here, the [key dates in 2020 are as follows](#), in order of earliest processing date:

| State | Processing Begins | Tabulation Begins | Ballot Receipt Deadline |
|----------------|-------------------|-------------------|-------------------------|
| Florida | Sept. 24 | Sept. 24 | Nov. 3 |
| North Carolina | Sept. 29 | Nov. 3 | Nov. 12 |
| Arizona | Oct. 7* | Oct. 20 | Nov. 3 |
| Michigan | Nov. 2 | Nov. 3 | Nov. 3 |
| Pennsylvania | Nov. 3 | Nov. 3 | Nov. 6 |
| Wisconsin | Nov. 3 | Nov. 3 | Nov. 3 |

* Arizona starts processing ballots as soon as they are received. The processing date shown is approximately when officials begin to mail out ballots.

Tabulating the Vote: Tabulating, also known as counting, is the next step. Tabulation usually begins on Election Day at the close of the polls, but some states begin the process earlier. States generally use machines to perform the initial count to prevent human error. The specific tabulation technology used in each state varies widely. Poll workers generally feed paper ballots into machines, which will print out a final count at the end of the day. Precincts are usually required to maintain and securely store or transfer to the county a paper record of votes, both the paper ballots cast and printouts of the aggregated initial counts, in case of a recount. States also have processes for interpreting ballots that are not legible to a machine, such as when a voter misspells the name for a write-in candidate, which can require manual counts by poll workers.

Reporting the Vote: Local election officials are typically required to submit their tabulations into a state's centralized results reporting system at a designated time on election night. In states that can start the process of tabulating ballots before Election Day, the first results revealed on election night are often results from early in-person voting and swiftly-retained mail-in ballots. Some states require election officials to work continuously until the initial count is complete.

Certifying the Vote: The initial results revealed on election night are verified over the coming weeks as election administrators complete an official canvass. Canvassing is the procedure through which election officials verify that each ballot cast in the election was correctly counted. During canvassing, the materials, equipment, and results of an election are reviewed, corrected, and officially recorded. The "canvass" is the official tally of votes for any given election. Once the canvass of the ballots is completed and any discrepancies resolved, the vote totals are then certified, usually by the Secretary of State. **Certification** is the process by which the results of an election are made official. Canvassing and certification are two closely related processes, and the terms are sometimes used interchangeably, but it is important to note that an election cannot be certified until a canvass is complete. Certification involves a presentation of all of the canvass documentation, including certified returns, statistics, and narrative to the canvassing board for their review and approval. Following the canvassing board's certification of the election, and if required by State law, the responsible election authority will provide each candidate with a notice of certification of the election. If candidates contest the results or the election is very close, the state may conduct a recount.

Together, these four steps constitute how American election officials count the vote. We examine six battleground states (Arizona, Florida, Michigan, North Carolina, Pennsylvania, and Wisconsin) below, describing in detail how each state performs this four-step process.

Arizona

Of the battleground states, Arizona is distinctive in that it allows early counting of ballots (including mail-in ballots), starting 14 days before the election. Partial results will be available on Election Day, despite the expected increase in mail-in ballots. Some Arizona election rules are still in [litigation](#), including the deadline for curing a mail-in ballot that has been returned with no signature and the treatment of provisional ballots cast in the wrong precinct. But it is unlikely that there will be any additional decisions in these cases before the election that impact how ballots are counted.

Processing Mail-In Ballots

Under Arizona law (Ariz. Rev. Stat. § [16-550](#)), early ballots can be opened and counted by election officials 14 days before Election Day, but officials may not release the results until all precincts have reported or until one hour after the polls close on Election Day. All mail-in ballots must be received by 7:00 PM on Election Day to be counted. A case filed in August, [Yazzie v. Hobbs](#), challenges this requirement that mail-in ballots be received by elections officials—rather than just postmarked—before 7:00 PM on Election Day, but a federal district court denied a preliminary injunction to stay the Election Day deadline, which denial was affirmed on appeal by the U.S Court of Appeals for the Ninth Circuit. So the Election Day ballot receipt deadline will stand for the election.

Mail-in ballots are certified through signature verification. Though such ballots cannot be counted earlier than 14 days before Election Day, they can be cleared through a [signature verification](#) process that begins when the ballot and ballot affidavit is received by the county recorder or official in charge of the election (approximately the week of October 12th this year, as ballots were mailed beginning [October 7th](#)). **The process involves comparing the signature on the ballot affidavit envelope with the signature on the voter's registration record.** If a signature cannot be verified because it is inconsistent with the voter's registration record, election officials are required to make “reasonable efforts” under Arizona Revised Statutes § [16-550](#) to contact voters and give them an opportunity to correct the signature. Voters will have until the fifth business day after the election to [correct](#) any mismatched signatures. If the signature on the ballot envelope is not [verified](#) by this time, the ballot is not counted. If the signature is [verified](#), the County Recorder will mark the unopened affidavit envelope as such and keep the ballot and affidavit unopened in the return envelope until they are transferred to the election officer for further processing and tabulation.

By contrast, if the ballot is missing a signature, voters have only until 7:00 PM on Election Day to fix the error before their ballot is rejected. Arizona law is silent on the procedure for missing

signatures (see Ariz. Rev. Stat. § [16-550](#)), but the current version of the [Elections Procedures Manual](#) does address this issue. [According to](#) the Manual, “[i]f the early ballot affidavit is not signed, the County Recorder shall not count the ballot. The County Recorder shall then make a reasonable and meaningful attempt to contact the voter via mail, phone, text message, and/or email, to notify the voter the affidavit was not signed and explain to the voter how they may cure the missing signature or cast a replacement ballot before 7:00pm on Election Day. The County Recorder shall attempt to contact the voter as soon as practicable using any contact information available in the voter’s record and any other source reasonably available to the County Recorder. Neither replacement ballots nor provisional ballots can be issued after 7:00pm on Election Day.”

The Arizona Democratic Party [sued](#) over this disparity in procedures. [Arizona Democratic Party v. Hobbs](#) challenges the current procedure that allows voters with mismatched signatures five days after the election to verify their ballots, while allowing those with missing signatures only until 7:00 PM on Election Day to fix their mistake. The Election Day deadline makes voters more likely to have their vote rejected, as they are far less likely to receive notice in time to correct the error. In addition, the inconsistency between the deadline for mismatched signatures and missing signatures could be a source of confusion for voters. The 9th Circuit has [put on hold](#) a federal district court order that would extend the deadline to address unsigned mail-in ballots, [pending appeal](#).

Ballots can also be rejected in the processing stage if they are cast in the wrong precinct. This rule has also generated litigation. In [Brnovich v. DNC](#), the plaintiffs seek to [eliminate](#) the requirement that ballots cast in the wrong precinct are automatically discarded and not counted, proposing instead that votes for county, state, and national offices on ballots cast in the wrong precinct should be counted but that votes for precinct specific offices should not be counted. The Ninth Circuit [struck down](#) the law, finding that it was enacted with the intent to discriminate against minority voters. But the Arizona [Attorney General](#) appealed the case to the Supreme Court of the United States, which granted certiorari and will [hear the case](#) in 2021; the law [remains in effect](#) until that time.

Tabulating the Vote

Logic and Accuracy Tests

Arizona requires all of its election equipment be tested and certified before an election. Under Arizona Revised Statutes § [16-449](#), this testing and certification process is to take place both before and after each election to ensure it is counting votes accurately and attributing them to the correct candidates and ballot measures. Each county is required to test all of its [election equipment](#) (i.e. voting machines) before any tabulation can begin. These tests must be [overseen](#) by at least two elections staff

or inspectors of different political parties. In addition, the testing must be to observation by representatives of political parties, candidates, the press, and the public. Additionally, for any election that includes a federal, statewide, or legislative office, the Secretary of State must conduct additional [logic and accuracy tests](#) on equipment from various counties..

Early Ballots

In-person [early voting](#) begins 27 days before Election Day and continues through the Friday before the election. The elections officer may begin tabulating early ballots after confirmation from the Secretary of State that all voting equipment passes any required logic and accuracy test. Ariz. Rev. Stat. § [16-552\(A\)](#). [Tabulation of early ballots can start 14 days before the election.](#) A.R.S. § [16-550\(B\)](#). Once the signature on an early ballot affidavit is verified by the County Recorder, the ballot is sent to the early ballot board, which is made up of staff members who are required to be affiliated with different political parties. [The early ballot board removes the ballots from their envelopes and transports them to the tabulation room where election officials run them through tabulators.](#) The ballot tabulation room is required by [law](#) to have live video feed so voters are able to watch ballot tabulation occur.

Election Day Ballots

Some counties use the [central count](#) method in which voters put their completed ballots in a “secured ballot bin” which is transported to the county’s ballot tabulation center after the polls close. This transportation is carried out by “election workers” of different political parties.

[Other counties use the precinct tabulation method, in which voters or poll workers feed the completed ballots into a tabulation machine located at the voting location.](#) The machine tabulates the ballots immediately and saves the vote count to a removable media device which is stored inside the tabulator. After the polls close, the poll workers or sheriff deputies bring the removable media device to the central counting location for the county. [At the central counting location, an election official loads the results from the removable media device into the secure election management system and combines the vote totals for all the polling locations.](#)

All counties must follow [chain of custody protocols](#). This includes requirements for documentation on the handling of every ballot, storage of ballots in secure locations, and the live video feed on the ballot tabulation rooms. Counties must also follow protocols for ensuring the security of all ballots, including the use of tamper-evident seals, identification badges, and having two or more election officials of opposing political parties present.

Reporting the Vote

Under Arizona Revised Statutes [Title 16 Section 623](#), unofficial tabulated results may be released after all precincts have reported or one hour after the closing of polls, whichever comes first. It appears that the latter is the de facto default, as the official [Secretary of State \(SOS\) website](#) indicates that the first results will be released at 8:00 PM, which is one hour after the polls close at 7:00 PM. These first results will include early ballots, such as mail-in ballots, which can be counted starting [14 days before election night](#). After that, these results will be updated “sporadically” as counties receive information from voting machines at their polling locations. [These results are unofficial](#), as they have not yet been certified by the board of supervisors or other officers in charge. Results are simultaneously [shared](#) with the SOS via phone, fax, or “other electronic means,” as they are tabulated at each precinct.

Arizona uses software from BPro, a private company that operates the TotalVote Election Software, for its state election night reporting system, which most counties also rely on to display their results for the public. On election night, the state updates election results on [its ENR website](#) as information is sent in from all counties. The state ENR website allows the public to view results by county, so 13 out of the 15 counties rely on this as their main ENR system. In most cases, the individual counties also upload results to their own websites as .pdf or .txt files. Two counties, [Greenlee](#) and [Pinal](#), use Scytl, another private company’s election software, to post their results on their individual county websites. Notably, while the “Precincts Reporting” number represents the “number of voting locations that have reported election results,” it is unclear if this means that the included precincts have finished tabulating their results or if they still have votes left to count.

Certifying the Vote

To [certify](#) the election results, election officials must canvass the election results of each precinct or election district. The Secretary of State Election Services Division is in charge of [certifying](#) on the state level while the Board of Supervisors for each county certifies the county. [The canvass verifies vote totals for all races tabulated by voting equipment as well as write-in votes](#). Canvassing must be carried out by a [Board of Supervisors](#) in a public meeting between six and [20 days](#) after the election. The Board of Supervisors is made up of [county officials](#) elected to a four-year term. The official election [results](#) must include a Statement of Votes Cast, a cumulative Official Final Report, and a Write-Ins Vote Report. [The Statement of Votes Cast must include the number of ballots cast in each precinct and county, the titles of offices up for election, the name of the people up for election, the number and title of each ballot measure, and the number of votes cast for and against each ballot measure](#). The cumulative [Official Final Report](#) must include the total number of precincts, total number of ballots cast, total number of registered voters eligible for the election, and number of votes cast for each candidate by district or division. The [Write-Ins Vote Report](#) must include the name and

number of votes for each authorized write-in candidate by precinct. Once the board of supervisors [completes](#) the election results certification, the Official Final Report and Statement of Votes Cast must be published on the website of the officer in charge of the election. Under Arizona Revised Statutes § [16-645](#), if the election includes a federal, statewide, or legislative office or a statewide ballot measure, the Board of Supervisors or elections officer in charge is required to [transmit](#) the official canvass to the Secretary of State electronically and by mail.

Florida

Understanding Florida's procedures for processing and counting vote-by-mail ballots is especially important, given the number of Floridians expected to vote by mail. In the 2016 and 2018 general elections, vote-by-mail ballots constituted approximately 30% of total ballots cast in Florida. This year, Florida voters [requested nearly 5 million](#) vote-by-mail ballots, approximately a 40% increase over the number of vote-by-mail ballots requested in 2016.

Florida's vote-counting process consists of opening the ballots, tabulating the ballots, reporting the results, and certifying the results. All tabulation systems used in Florida must undergo a rigorous Logic & Accuracy test before public use. While the state's process bears general similarities to that of other states, some salient features of Florida's vote-counting process include its voter signature verification process and its tabulation system approvals process.

Processing Mail-In Ballots

The timeline and procedure for opening and counting mail-in ballots is specified under Florida Statutes Title IX [§§101.657, 101.68](#). Signature verification and counting [can begin](#) at 7:00 AM on [October 12, 22 days before Election Day](#); releasing the results early is a felony. However, earlier this year, in response to the COVID-19 crisis, Florida Governor Ron DeSantis issued an [Executive Order](#) that permitted Florida counties to begin processing and [tabulating vote-by-mail ballots immediately after the tabulation machines have completed the public Logic & Accuracy tests](#) (described below). Therefore, because the Florida Supervisors of Elections [began sending mail-in ballots](#) to voters on September 24, a county could, in theory, begin counting mail-in ballots on September 24, so long as its tabulation machines had been certified. Also, counties cannot begin tabulating the vote *later* than noon on the day following the election.

[In processing mail-in ballots](#), the canvassing board must compare the voter's signature on a mail-in ballot envelope with the voter's signature in the precinct register to see that the voter is

registered in the county and to determine the legality of that vote-by-mail ballot. The canvassing board can only determine that the signatures do not match if a majority of the canvassing board arrives at that conclusion and if the signature mismatch is “beyond a reasonable doubt.” The supervisor must then notify the voter as soon as possible, both by first-class mail and by email, text message, or telephone. To cure the defect, the voter must submit a cure affidavit, certifying that they submitted their vote-by-mail ballot and attaching documents that confirm their identity. The voter has until 12:00 PM on the second day after the election to either mail or email their cure affidavit to the county supervisor of elections.

A recent [empirical study](#) on uncounted mail votes in Florida (based on reasons such as lateness or signature mismatches) reveals statistically significant differences in rejection rates among various cohorts of the population. For instance, in 2018, Jefferson County rejected 0% of its mail ballots while large counties like Broward and Miami-Dade rejected nearly 3%. One reason for this difference in rates among counties is an inconsistency in how various counties process ballots. For instance, different elections offices in Florida use [different methods](#) to contact voters to cure their ballot. Some counties contacted voters over the phone, by email, and even through Facebook, while other offices simply mailed a notice. A federal judge [called](#) Florida’s statute governing rejected vote-by-mail ballots “a crazy quilt of conflicting and diverging procedures” with the “canvassing boards across the state employing a litany of procedures when comparing signatures.”

Once the supervisor of elections confirms that the signature on the voter’s ballot envelope or the cure affidavit matches the voter’s record, the voter’s ballot envelope is opened. The election staff will then mix the enclosed secrecy envelopes to make it impossible to determine which secrecy envelope came out of which signed mailing envelope. The county is then ready to tabulate the vote.

Tabulating the Vote

Florida precincts tabulate their votes using machine counting systems that digitally scan voter ballots, capture voter selections, and enable precincts to evaluate and download the aggregate results. Under Florida Statutes [Title IX Chapter 101](#), all voting systems used for tabulation must be certified by the State. As a threshold matter, voting systems must meet various hardware and software requirements set forth in [§101.5606](#). For instance, among other requirements, a voting system must be capable of automatically producing precinct totals in printed form.

A voting system must also undergo a rigorous public “[Logic & Accuracy \(L&A\) Test](#)” under [§101.5612](#). For any given precinct, the canvassing board can publicly test either all or a subset of voting systems used in the precinct. In this public test, officials use a “test deck” set of ballots that model real ballots voters may use in casting their vote. For instance, the test deck uses actual ballots that are

hand-marked or marked with balloting devices. This test deck is run through the voting system. If a tested tabulation device produces an error in tabulating the test deck, the device is deemed unsatisfactory. The canvassing board must then determine the cause of the error; identify and test other devices that could reasonably be assumed to have the same error; and test a sufficient number of devices to determine that all other devices are satisfactory.

The canvassing board must keep records for all of the public L&A tests. Currently, all certified voting systems are listed on the Florida Division of Elections [website](#), along with each system's corresponding certification memos and certification test reports. [Democracy Suite](#) and [EVS](#) are the two certified tabulation systems being used in Florida. Democracy Suite is used by 30 States, and EVS by more than 40 States.

Finally, according to [Florida Statutes Title IX Chapter 102](#), results of all tabulated early voting and absentee voting must be entered into the county's election management system. [The county's election management system is responsible for aggregating data on verification, tabulation, and reporting, and it enables the county to export that data and to view ballot images.](#) All early and absentee ballots that have been tabulated and canvassed must be entered into the system by 7:00 PM the day before the election as unofficial results. These results must remain private until the close of the polls on Election Day.

Reporting the Vote

Election Night Reporting (ENR) procedures for Florida are dictated by Florida state law, though the specific reporting mechanisms can vary by county. As discussed above, while counties must tabulate early voting by 7:00 PM the day before the election, it is illegal to publicize these results at this time. Results must be reported to the Florida Department of State (DOS) 30 minutes after polls close and are subsequently updated every 45 minutes "in a format prescribed by the DOS". All results must be submitted to the DOS by noon on the fourth day after the election.

On election night, voters can visit a homegrown site, [Florida Election Watch](#), to view results, though the vast majority of counties use a commercial product from the company VR Systems for election night results. VoterFocus, the Election Management System (EMS) developed by VR Systems, is used by [65 of 67 counties](#) in Florida (it appears that [Palm Beach County](#) has recently also adopted VoterFocus). While the Democracy Suite and EVS hardware and software packages are responsible for tabulating the ballots, the VoterFocus software is responsible for organizing and managing election data. The election night results component reports votes per candidate (which can further be broken down into Vote By Mail, Early Voting, and Election Day) and results by precinct. [Sarasota County](#) uses the ENR system from Scytl, another large voting technology company, while [Orange County](#) appears

to post its results on its website as .xls files. All counties simultaneously report their results to the Florida Department of State to update the state's Florida Election Watch website.

Florida has official processes for correcting reporting errors and responding to close results. As dictated in [Florida Statutes Title IX Chapter 102 Section 6](#), if “unofficial returns”—votes that have been canvassed but not certified—contain any counting errors, counties must correct the errors and retabulate. The DOS will then verify the tabulation and compare the tabulation software with the software “filed with the department,” thus checking that both the results and the software the results are counted accurately. Critically, if unofficial results indicate that a candidate or ballot measure has lost by less than 0.5%, a recount is ordered of the votes for that specific election. Moreover, if the margin of victory is equal to or less than 0.25 percent, the recount must be performed manually.

Certifying the Vote

Florida has different timelines for counties to submit their unofficial election results and to certify their official election results. Under Florida Statute Title IX [§ 102.141\(5\)](#), all Florida counties must submit *unofficial* results to the DOS by noon on the fourth day after the election. Under [§ 102.112\(2\)](#), counties then have until 12 days after the general election to canvass and certify their *official* results to the DOS.

Once counties have canvassed and certified their results, the [Florida Elections Canvassing Commission](#), made up of the governor and two members of the cabinet selected by the governor, certify all of the counties' votes. The state Canvassing Commission convenes at 9:00 AM 14 days after the general election to certify all of the votes. If, within five days after the certification of votes by the Elections Canvassing Commission, a county canvassing board determines that it has found an error in the official returns it reported to the state, and that a correction of that error could result in a change in the outcome of an election, the county canvassing board must certify corrected returns to the Department of State within 24 hours. The Elections Canvassing Commission must then correct and recertify the election returns as soon as practicable.

Michigan

Michigan officials are [anticipating a record-breaking](#) number of ballots this year, with mail-in ballots expected to comprise [60-70%](#) of all votes in the state. [The COVID-19 pandemic is expected to put immense strain on Michigan's election system, with the number of absentee ballot applications on track to hit 350% of the number of absentee ballots from 2016.](#) Furthermore, since the 2016 election, Michigan has greatly expanded voting accessibility. In 2018, voters passed a series of [statewide ballot](#)

[proposals](#) allowing all eligible and registered Michigan voters to request an absentee ballot without providing a reason and allowing same-day voter registration.

In 2016, Republican presidential candidate Donald Trump won Michigan by a [little over 10,000](#) votes, capturing the state by the narrowest margin of any state in the country. Given that the election results are expected to be [hotly contested](#) in court, a possible order to recount the votes in Michigan could prove to be an incredibly complicated endeavor. Precincts with ballot count totals that are different from their result totals [are ineligible](#) to be recounted. This is not usually a major problem, except for the fact that voting centers are expected to grapple with incredibly high absentee voting, introducing opportunity for error. In Detroit, for example, [72% of voting centers](#) during the August 4th primary reported inaccurate ballot counts. Marking these precincts as ineligible for recount could have a significant impact in the event of a close race.

Processing Mail-In Ballots

Under [MCL §168.764a-b](#), voters must submit their marked absentee ballots [before polls close](#) on November 3rd, either by mail or hand-delivered to their city or township clerk. While an initial ruling by the Michigan Court of Claims extended the deadline, allowing all mail-in ballots [that arrive within two weeks of Election Day to be counted](#), the Michigan Court of Appeals [overturned the decision](#), stating that there was no need for the extension given the number of ballot delivery options available to voters.

Once election precincts receive their absentee ballots, they can employ one of two options: (1) the clerk may deliver the ballot to the absent voter's precinct, where it will be processed and counted by election inspectors, MCL 168.765, or (2) if the city or township election commission has established an absent voter counting board (AVCB), then the ballots must be taken to the AVCB for processing and counting, [MCL 168.765a, 168.765d](#). AVCBs are dedicated [election counting boards](#) that meet at a separate location away from the polls and focus solely on processing absentee ballots under the supervision of election inspectors. For reporting purposes, AVCBs are precincts, so their results are reported separately from the precincts established for in-person voting. In contrast, ballots delivered directly to the absent voter's precinct are included as part of the precinct's total ([Elec. Offs. Manual, Ch. 8](#)). On June 23, 2020, Governor Gretchen Whitmer [signed into law](#) an amendment that gives municipalities the option to combine resources with other cities and townships in the county to create AVCBs, whereas the law had previously only allowed AVCBs to serve an individual precinct.

According to [MCL §168.765a\(8\)](#), absentee ballots cannot be processed until 7:00 AM on Election Day. A bill with bipartisan support was [just signed into law](#) on October 6th, 2020, expanding work shifts for absentee ballot counting and [allowing municipalities](#) with populations of at least 25,000 to process absentee ballots the day before the election, from 10:00 AM to 8:00 PM. Processing

a mail-in ballot [requires](#) satisfaction of various formalities, including that the clerk has completed relevant portions of the return envelope and that the ballot stub number matches the number recorded for that voter. [According to MCL §168.766](#), the board of inspectors must then verify the voter's signature on the ballot envelope against their signature in the qualified voter file, registration record, or master card (depending on their method of voter registration). See the [Healthy Elections Signature Verification report](#) for more details on Michigan's verification process. If the signature is verified, the ballot is then removed from its exterior mailing envelope and the ballot 'processing' is complete. In Ann Arbor, MI, processing a single ballot takes an estimated [45 seconds](#).

Only after a mail-in ballot has been fully processed [can it be removed](#) from its secrecy envelope and placed into a tabulator for counting. Under [MCL §168.798c\(1\)](#), absentee ballots may be cast as paper ballots, ballot cards, or a combination thereof, depending on the precinct. If an absentee voter submits a paper ballot, election inspectors are authorized to record the ballot on a paper ballot card that is then fed into the tabulator. These tabulators must automatically reject ballots that are 'overvoted' or blank per [MCL §168.795\(2\)](#) (consistent with tabulators used for in-person voting described in the next section). Per [MCL §168.809\(2\)](#), after the precinct or AVCB completes its vote count, a sealed statement of returns is reported to the county clerk, who may then provide an unofficial tabulation of the returns to the public, pending an official canvass by the county canvassing board.

Tabulating the Vote

Each Michigan county has the discretion to choose its own electronic voting system, so long as it meets all of the rigorous requirements outlined in [MCL §168.795\(1\)](#). The statute states the system must include: (1) usage of paper ballots for tabulating purposes([§168.795\(1\)\(b\)](#)); (2) electronic tabulation equipment that automatically rejects all choices recorded on an elector's ballot if the elector votes for more choices than they are allowed to (also known as overvoting)([§168.795\(1\)\(c\)](#)); (3) electronic tabulating equipment that can reject a ballot if no valid votes are cast([§168.795\(1\)\(g\)](#)); and (4) electronic tabulation equipment that can alert the elector if their ballot is spoiled and give them the opportunity to cast another ballot([§168.795\(1\)\(c\)](#)). Additionally, the tabulators should also provide a method for them to be rendered 'inoperable' if vote totals are revealed before polls close per [§168.795\(2\)](#). Under [MCL §168.803\(2\)](#), a vote will count only if the voter places a mark properly in the predetermined area. Lastly, if, for whatever reason, the counting center is separate from the precinct, and a ballot being fed into the tabulator is rejected because of physical damage or defect, election officials can duplicate the damaged ballot and re-feed it into the tabulator [under MCL §168.798a](#). There are currently [three companies](#) that supply tabulators that meet these requirements to the state.

Every electronic tabulating system is tested at least twice under Michigan law. According to the [Test Procedure Manual](#), both tests must confirm that ["1\) the equipment is performing properly, 2\) the](#)

ballots have been properly prepared for each precinct, and 3) that the programs will accurately count votes.” The first test is known as the “preliminary accuracy test” and must be run as soon as clerks receive the tabulator and ballots. The second test, known as the “public accuracy test,” is mandated by [MCL §168.798\(1\)](#). Election officials must give the public at least 48 hours notice of the time and place of the test, and such notice must be placed in a newspaper “published in the county, city, village, township, or school district where the electronic tabulating equipment is used.” Both of these run a series of ballots through the tabulator, checking to make sure that the tabulator accurately counts the ballots and rejects ballots that are blank or overvoted as outlined in [MCL §168.795\(1\)](#).

Under [MCL §168.798b](#), once the vote count is fully tabulated and write-in and absentee votes are separately added (if necessary), the count reported by the electronic tabulating equipment constitutes the official return of each precinct or election district, once it has been duly certified.

Reporting the Vote

Michigan state law requires county clerks to tabulate unofficial results and report them to the public upon receipt of statement of returns. According to [MCL §168.798b](#), unofficial results of Michigan elections must be made available to the public. Additionally, according to [MCL §168.809](#), upon receipt of the sealed statement of returns from the county election inspectors, county clerks must compile unofficial results for the county and make them available to the public. However, no timeline is placed on the public reporting requirement by law, so while unofficial results are often available on election night, counties seem to publicly post unofficial results anywhere from hours to months after the close of polls.

Election night results are reported at the state and local level in Michigan. The Michigan Secretary of State’s office reports unofficial results on its webpage. Many counties also directly post their unofficial results on their designated websites as PDFs. A list of those county websites can be found [here](#). Additionally, a few counties employ [ElectionSource](#), a local Michigan company, as an Election Management Service (EMS) vendor. ElectionSource provides an unofficial results reporting site for county-level results, found [here](#). However, Michigan’s largest county, Wayne County, cut ties with ElectionSource’s results reporting service shortly before the 2018 general election, due to [operational mishaps](#) during the 2018 primary.

Certifying the Vote

Each of Michigan’s 83 Boards of County Canvassers [is responsible](#) for certifying its county’s votes to the [Michigan Board of State Canvassers](#). Under [MCL §168.822](#), a Board of County Canvassers must certify that county’s votes within 14 days of the election. Once a county has finished

its certification, then, under Michigan Coded Laws [§168.824](#), it must prepare a sealed statement containing data on the county's votes, including, for instance, the number of votes cast for each office. If the Board of County Canvassers fails to certify its votes and prepare this sealed statement within 14 days, it must deliver all relevant voting records on hand to the Board of State Canvassers, and the Board of State Canvassers will finish certifying that particular county's votes within 10 days of receiving those records. Under [MCL §168.842\(1\)](#), the Board of State Canvassers must begin the state certification process within 20 days after the election and finish certification within 40 days after the election.

Michigan can also require counties to certify their votes on an expedited basis. Under [MCL §168.842\(2\)](#), if the unofficial election returns show that the vote differential between the first place and second place candidates for the presidential election is fewer than 25,000 votes, the secretary of state may direct the Boards of County Canvassers to finish certification more quickly. In fact, the secretary of state may require the Boards of County Canvassers to finish certification and prepare their sealed statements between 7 and 14 days after the election.

Candidates can also petition the Michigan secretary of state to conduct a vote recount in certain counties. Under Michigan Coded Laws [§168.879](#), the candidate must petition for a recount within 48 hours of the completion of certification. The candidate must be able to allege a good-faith belief that, but for voter fraud or mistake, the candidate would have had a reasonable chance of winning the election. The petition must allege specific instances of wrongdoing, if the candidate has such evidence, but the candidate must specify the counties in which they request a recount. Under Michigan Coded Laws §§[168.867](#) and [168.881](#), the candidate requesting a recount must pay \$25 deposit per precinct. This fee is raised to \$125 per precinct if the pre-petition margin of victory for the winning candidate over the petitioner is greater than 50 votes, or 0.5 percent of all votes cast, whichever is greater. If the outcome of the election is altered as a result of the recount, the deposit is refunded. Notably, under Michigan Coded Laws §§[168.880](#) and [168.880a](#), registered voters in Michigan can also petition for a vote recount and the state itself will automatically trigger a statewide recount if the winning candidate's lead is 2,000 votes or fewer.

North Carolina

The way North Carolina processes and counts its mail-in ballots may have a profound effect on the results of the state's 2020 General Election. [As of September 30, 2020, North Carolina had already experienced an approximately nine-fold increase in absentee ballot requests over the number requested at the same date in 2016.](#) North Carolina election law allows officials some flexibility to deal with this influx. For instance, local election officials have the authority to begin [opening](#) and preparing absentee ballots for counting on the fifth Tuesday before Election Day. They may also hold additional meetings

after Election Day and prior to the day of canvass to [count](#) late-arriving absentee ballots. Recent litigation has also [changed](#) the procedures for how absentee ballots can be processed and counted. The outcome of pending litigation, including [filings](#) with the U.S. Supreme Court, may further alter how North Carolina can process and count its absentee ballots.

Although some aspects of North Carolina election law require statewide uniformity, others allow a degree of discretion for individual counties. North Carolina statute lays out some [general principles](#) for how ballots should be counted. It also requires the North Carolina State Board of Elections to adopt [uniform](#) standards and procedures for how counties should count votes and how individual counties may make use of [different](#) vote-counting systems, such as electronic, mechanical, or hand-to-eye counts. All counties may be required to [engage](#) in hand-to-eye counts or recounts of at least some of their paper ballots or records. The results from all counties will be [viewable](#) on election night on the North Carolina Election Results Dashboard. Later, the canvassing and certification of votes [takes](#) place both at both the county- and state-level, with the potential for mandatory and discretionary recounts to [delay](#) the completion of the canvass at each level.

Processing Mail-In Ballots

North Carolina election law and guidance provide flexibility for county boards of elections to deal with the anticipated significant increase in mail-in ballots. Before beginning to count mail-in ballots (which North Carolina election officials often [refer](#) to as “absentee ballots”), county boards of elections may begin [scanning](#) each approved absentee ballot, a process which consists of opening approved absentee ballots, removing them from their envelopes, and inserting them into the tabulator. At this time, the county boards [may](#) use the tabulators to “read” the ballots, but the tabulators do not count the ballots until Election Day. This early preparatory step allows election officials to [identify](#) which ballots cannot be read by the tabulator machine, perhaps because of damage, and to make duplicate copies of the unreadable ballots that can be read by the tabulator machine. That way, election staff can [avoid](#) having to manually input each voter’s selections from a ballot into the reporting software, which can save time come Election Day. All approved absentee ballots must be [scanned](#) by the tabulator machine. Each county board of election can [decide](#), by majority vote, to begin the scanning process during each absentee board meeting. Indeed, a September 22, 2020, [memo](#) from North Carolina State Board of Elections Executive Director Karen Bell notes that, due “to the significant increase in absentee ballots this election, it is strongly recommended that county boards authorize the scanning of approved ballots during absentee board meetings instead of waiting until Election Day.” The earliest county boards can [begin](#) scanning absentee ballots is thus during the first absentee board meeting, which county boards are required to hold on September 29 for the 2020 general election. County boards also [have](#) the authority to delegate additional preparatory steps to staff to perform before absentee board meetings. Preparatory steps [include](#) tasks such as inspecting the

ballot return envelopes for deficiencies and, if any deficiencies are discovered, notifying voters within one business day.

The process for how county boards and their staff can evaluate and address deficiencies in absentee return envelopes has been the subject of recent litigation. The aforementioned September 22, 2020 memo from the North Carolina State Board of Elections, for instance, is at issue in the lawsuit [*Arnett v. North Carolina State Board of Elections*](#), which may require the State Board to provide greater access to the public to observe and provide input to the absentee return envelope evaluation process. An August 2020 [memo](#) from North Carolina State Board of Elections Executive Director Karen Bell, later revised in September and October following a recent settlement and rulings in [*N.C. Alliance for Retired Americans v. North Carolina*](#) and [*Democracy NC v. North Carolina State Bd. of Elections*](#), also provides guidance on how the county boards and their staff can evaluate and address deficiencies in absentee return envelopes. Notably, in verifying the voter's signature on the return envelope, the county board should [presume](#) that the signature is that of the voter, absent clear evidence to the contrary, if "it appears to be the name of the voter." Furthermore, the signature will be [accepted](#) even if it is illegible. There is also no legal requirement to [compare](#) the voter's signature on the absentee return envelope "with the voter's signature in their registration record." If an absentee return envelope [lacks](#) a witness signature, however, then a voter can no longer cure the deficiency and save the ballot by submitting a certification over mail or email. Instead, their ballot will be rejected and county boards and their staff will [reissue](#) the voter a new ballot.

Other recent litigation, *Wise v. North Carolina State Board of Elections* and *Moore v. Circosta*, has challenged the State Board's rules for evaluating and addressing deficiencies in absentee return envelopes as outlined in its August 2020 [memo](#) (revised in October), as well as its revision of the absentee ballot deadline. Initially, on October 3, a U.S. District Court for the Eastern District of North Carolina, Western Division [issued](#) a temporary restraining order preventing the State Board of Elections from enforcing [rules](#) for evaluating and addressing deficiencies in absentee return envelopes, and transferred both cases to the U.S. District Court for the Middle District of North Carolina. Later, on October 14, the latter court then [denied](#) the conversion of the temporary restraining order into a preliminary injunction. Then, on October 20, the U.S. Court of Appeals for the Fourth Circuit [denied](#) plaintiffs' appeals and their requests for injunctive relief. As such, the State Board can continue to enforce the rules for evaluating and addressing deficiencies in absentee return envelopes that it outlined in its recent [memos](#), and absentee ballots can be [received](#) and counted nine days after Election Day, so long as they are mailed on or before Election Day. Plaintiffs in both cases [filed](#) a request with the U.S. Supreme Court for an emergency injunction, but on October 28, the Court [denied](#) the request. However, the Supreme Court may decide to revisit the issue after the election, thus leaving open the possibility that mail-in ballots postmarked on Election Day but received more than three but less than nine days after Election Day may become invalidated at a later date.

Pending further action by the U.S. Supreme Court, the State Board can continue to enforce the rules for evaluating and addressing deficiencies that it outlined in the version of its August 2020 [memo](#) that it revised in October 2020. Generally speaking, some deficiencies can be cured by the submission of a certification from the voter addressing the deficiency, whereas other deficiencies require the reissuance of a ballot, and still others require board action. If a deficiency is [discovered](#) in a board meeting, then it cannot be resolved by staff and will instead require board action to evaluate the deficiency. If the board [rejects](#) the envelope by majority vote, then it must notify the voter within one business day. If the envelope [indicates](#) that the voter is requesting a replacement ballot, lacks the signature of a witness or assistant, or is unsealed when it arrives at the county board office, then staff will reject the ballot and reissue a new ballot along with a notice to the voter within one business day. By contrast, the following deficiencies can be [fixed](#) by sending the voter a cure certification through mail or email to provide them an opportunity to address it:

- Voter did not sign the Voter Certification
- Voter signed in the wrong place
- Witness or assistant did not print name
- Witness or assistant did not print address
- Witness or assistant signed on the wrong line

Although North Carolina election law does not allow county boards of elections to begin counting mail-in ballots until Election Day, it does provide some flexibility to allow additional time for counting. Under N.C. Gen. Stat [§163-234](#), each county board of elections is required to meet at 5:00 PM on Election Day to begin counting all mail-in ballots, except for late-arriving ballots or those challenged before 5:00 PM on Election Day. However, [§163-234](#) also allows county boards to begin counting absentee ballots from uniformed officers and overseas voters as early as 9:00 AM on Election Day. In addition, [§163-234](#) allows county boards to begin counting other mail-in ballots as early as 2:00 PM on Election Day, as long as they adopt a resolution at least two weeks prior to Election Day that states the place and time they will begin counting.

Election law also provides county boards of elections additional time to deal with an influx of late-arriving absentee ballots. For instance, county boards of elections can [adopt](#) a resolution to hold additional meetings after Election Day and before canvassing to count absentee ballots. If a county board adopts such a resolution, then [§163-234](#) requires them to publicly publish its contents. [§163-234](#) also requires county boards to meet after Election Day and before the start of canvassing to determine if all late-arriving absentee ballots have been assessed and counted. Any late-arriving ballots not [counted](#) before the day of canvass will be counted on the day of canvass.

Finally, North Carolina election law allows some flexibility in who can count absentee ballots, even while setting requirements for how they can count them. Each county board of elections [may](#) hire staff to help them count the absentee ballots, but must observe and supervise the staff. As staffers open each ballot envelope, the county boards will [record](#) the names of each voter in a paper or computer pollbook, then place each ballot in the appropriate box according to ballot type. Only after all ballots have been placed in their respective boxes can the counting process [begin](#).

Tabulating the Vote

North Carolina election law lays out the requirements regarding the timing and organization of the counting of ballots. Under [§163-182.2](#), vote counting at each precinct begins immediately after the closing of its polls on Election Day and continues until it is completed. [§163-182.2](#) also requires that vote counting in each precinct be conducted with the participation of precinct officials from all political parties present. In addition, it [allows](#) for any member of the public to witness the counting process but forbids them from participating or otherwise interfering.

[§163-182.1](#) lays out some of the general principles and rules for counting ballots. For instance, under [§163-182.1](#), no ballot can be rejected because of technical errors made in marking the ballot, unless it is impossible to determine the voter's choice. Furthermore, if a ballot is [rejected](#) by a scanner or other counting machine but election staff can clearly discern the voter's choice, then the ballot will be counted by hand. In addition to the general principles provided directly in the statute, [§163-182.1](#) requires the North Carolina State Board of Elections to adopt "uniform and nondiscriminatory procedures and standards" for vote counting. These include rules such as [08 NCAC 06B.0105](#), which indicates that provisional ballots will be counted before canvass. [08 NCAC 06B.0105](#) also prohibits county boards from discarding a voter's entire ballot if they are ineligible to vote for some items on the ballot; boards are required to count the items for which the voter is eligible.

Although counties may make use of different vote-counting systems, all counties may be required to engage in hand-to-eye counts of at least some of their paper ballots or records. [§163-182.2](#) notes how, in addition to hand-to-eye counts of paper ballots, counties may make use of "any certified mechanical or electronic voting system," including optical scan and direct record electronic voting systems. **Any counties that use a system other than hand-to-eye counts of paper ballots, however, are required to [hold](#) a hand-to-eye count of a random sampling of their paper ballots.** The sampling may [include](#) all paper ballots from one or more precincts, mailed absentee ballots, and ballots from early voting sites (where absentee voters are allowed to vote in-person before Election Day). It [must](#) also be of sufficient size to produce a statistically significant result. If there is a "[material discrepancy](#)" between the mechanical or electronic count and the hand-to-eye count, and there is no reason to doubt the accuracy of the hand-to-eye count, such as because paper ballots have been lost or destroyed, then the

hand-to-eye count takes precedence. If the discrepancy is “[significant](#),” then a complete hand-to-eye count will be conducted.

Reporting the Vote

The process for reporting the unofficial results is straightforward. After the counting is completed at the precincts, the chief judge or someone he or she designates will verbally [announce](#) the precinct’s unofficial results. Following the requirements of the recently rewritten [§163-182.2](#), precinct officials will then transmit the results in an unofficial report to the county board of elections as quickly as possible. This unofficial preliminary report will [include](#) the number of provisional ballots cast in that precinct and will not have a binding effect on the official county canvass. Immediately after the precinct reports are received, the chair, secretary, or their designee will [publish](#) the unofficial results to the news media.

County boards are in charge of reporting election returns. Under [§163-132.5G](#), county boards are required to report returns by precinct within 30 days after the election. The 30-day deadline does not, however, “[relieve](#) the county board of the duty to report returns as soon as practicable after the election.” North Carolina State Board of Elections Executive Director Karen Bell [extended](#) the reporting deadline of [§163-132.5G](#) by an additional 30 days, effective March 20, 2020, but her emergency amendment authorizing the extension [expired](#) in June 2020. In reporting the returns, the county boards must also [report](#), by precinct and by ballot item in each precinct, how many voters did not select any choice for a ballot item and how many voters selected too many choices for a ballot item.

On election night, the State Board of Elections will maintain an Election Results [dashboard](#). The dashboard will be updated as precincts report results to the State Board of Elections (SBE) and [will include data](#), in the form of maps, tables, and charts, and enable visitors to download election results spreadsheets. After polls close, the state expects to update the [dashboard](#) every 5-10 minutes.

Certifying the Vote

Under [§163-182.5](#) and [§163-182.6](#), canvassing and certification take place at both the county and state level. At the county level, each county board of elections will [meet](#) at 11:00 AM 10 days after the election to conduct the official tally of votes (or canvass) in precincts in that county and to ensure that all votes have been counted and tabulated correctly. If the initial canvass has not been completed by that time, the board may [hold](#) the canvass meeting at “a reasonable time thereafter.” After completing the canvass, the county board will prepare “abstracts” (defined under [§163-182](#) as “a document signed by members of the board of elections showing the votes for each candidate”) in the uniform format [requested](#) by the State Board of Elections. The abstract, at a minimum, [states](#) each

candidate's name and the number of votes received. Each county board [prepares](#) three originals of the abstract, retaining one for itself, submitting one to the clerk of the superior court for that county, and submitting one to the State Board of Elections. Six days after the completion of the canvass, if there is no election protest pending, then the county board will [issue](#) a certificate of election.

At the state level, the State Board of Elections will [meet](#) at 11:00 AM on the Tuesday three weeks after Election Day to complete its statewide canvass and ensure that the votes have been counted and tabulated correctly. If, at the time of its canvas meeting, the State Board has not yet received abstracts from some county boards, the State Board can temporarily [adjourn](#) the meeting for up to 10 days while it obtains the missing abstracts. In obtaining the abstracts from the county boards, the State Board is [authorized](#) to obtain one of the triplicate originals at the expense of the counties. Immediately after completing the canvass, the State Board will prepare two original copies of its composite abstracts, retaining one for itself and submitting the other to the Secretary of State, which the Secretary is then [required](#) to keep accessible to the public. Six days after the completion of the State Board canvass, if there is no election protest pending, then the State Board will [issue](#) a certificate of election.

Recounts have the potential to delay the completion of a canvass, and there are two types: discretionary and mandatory. When necessary to complete its canvass, the State Board has discretion to [order](#) a recount, and a county board may do the same if the State Board has not already [denied](#) a recount in that county. A losing candidate on a statewide ballot has the right to [demand](#) a recount if the margin of votes between the losing and the prevailing candidate is less than 0.5% of the votes cast or fewer than 10,000 votes. If the losing candidate wants to exercise this right, they must submit their [demand](#) in writing to the State Board by “noon on the second business day after the county canvass.” If the Executive Director later revises the initial results and concludes that the winning margin qualifies the losing candidate to demand a recount, then the Executive Director is [required](#) to notify the losing candidate immediately. After being notified, the losing candidate has 48 hours to [exercise](#) the right to a recount.

Candidates [have](#) the right to demand an *additional* recount following an initial recount if the initial recount did not use hand-to-eye counting and did not reverse the results for the losing candidate. In these circumstances, the losing candidate may, within 24 hours of completion of the initial recount, [demand](#) a hand-to-eye recount in a sampling of precincts. If the initial recount was not hand-to-eye and it does overturn the election results for the candidate who had initially been declared the winner, then that candidate [has](#) the same right to a hand-to-eye recount in a sampling of the precincts. Such a sampling must [include](#) all ballots in 3% of the precincts casting votes in each county, rounded up to the nearest whole number of precincts. For the purposes of this calculation, each one-stop (early) voting site would [be](#) considered a precinct. If extrapolating the discrepancy between the initial recount and the hand-to-eye recount in the sampling would [lead](#) to a reversal of the election results, then the State

Board of Elections will order a hand-to-eye recount in the entire jurisdiction in which the election is held.

Pennsylvania

The large number of absentee ballots expected in Pennsylvania, combined with legal requirements that prohibit processing them before Election Day, will make it difficult for Pennsylvania to announce results on election night. In 2019, a law was passed allowing all voters to vote-by-mail without providing an excuse. **As a result of this new law and the change in voting intentions due to the pandemic, a record number of voters plan to vote-by-mail in 2020.** Pennsylvania does not permit the tabulation of mail-in ballots to begin until after the close of polls on Election Day. That may mean no one will know the result of that critical state's election until days after the election, [depending](#) on the results of a few key counties. In fact, after the [primaries](#) in June, around half of the state's counties were still tabulating votes a week later.

The tabulation and canvassing system in Pennsylvania is fairly standardized. [District](#) level tallies are physically delivered to county offices, where they are aggregated, along with mail-in ballots and provisional ballots. Discrepancies and challenges over provisional ballots are reconciled and decided on at the [county](#) level. As the returns come in to the counties and as counties process mail-in ballots, they [report](#) the unofficial count to the Department of State. The unofficial counts are updated on the statewide election night reporting site. The third [day](#) after the election, the counties begin canvassing returns, once the official count is certified, a sealed copy is physically [delivered](#) to the Department of State.

The scope and process for counting mail-in ballots in Pennsylvania ([Title 25 P.S.](#)) has changed significantly in the past year. **[Act 77](#), passed by the state legislature in October 2019, expanded vote-by-mail to anyone who requests a ballot.** The law also centralized the processing of mail-in ballots at the county level. [Act 12](#), passed in March 2020, [responded](#) to COVID-19 public health concerns during the primaries and updated the procedural timeline for pre-canvassing and canvassing mail-in ballots. Subsequent to those changes, the Pennsylvania Supreme Court in September ruled on [Act 77](#) ([\[J-96-2020\]](#) and [\[J-97-2020\]](#)) by extending the period mail-in ballots can be received to three days after the election and allowed secure drop-off locations for mail-in ballots. On October 19, 2020, the U.S. Supreme Court [let stand the ruling](#) that Pennsylvania can count ballots received after Election Day. **The state supreme court has also ruled that the state cannot count mail-in ballots sent in without their state-provided inner envelope (referred to as a "secrecy envelope") intended to protect the privacy of mail-in votes. (Ballots without the "secrecy envelope" are sometimes referred to as "naked ballots.")**

These changes may have a significant impact on the results of the November 2020 election in this key swing state.

Processing Mail-In Ballots

The county boards of election are responsible for processing mail-in ballots. They cannot begin opening and counting ballots until the morning of Election Day and can record and publish results only after the close of polls. Pre-canvassing, the process of inspecting, opening, and taking ballots out of their inner “secrecy envelopes,” may begin once polls open on Election Day, at 7:00 AM (25 P.S. §3146.8(1.1)). After the polls close at 8:00 PM, counties can begin canvassing (counting) all ballots, and this process continues until all valid mail-in ballots have been counted (25 P.S. §3146.8(2)). Notably, the recent Pennsylvania Supreme Court ruling allows for ballots sent on Election Day to be counted so long as they are received within three days after Election Day and there is no evidence that they were mailed after Election Day. In addition, military ballots received seven days after Election Day can be counted and, thus, the pre-canvassing and canvassing period must continue until at least eight days after the election. The main difference between pre-canvassing and canvassing is that pre-canvassing begins before the polls close and canvassing begins after the polls close. It is only after polls close that the vote counts can be recorded or published (25 P.S. §3146.8(2)). Once canvassing starts, the county board meets to verify and tabulate ballots, with one representative from each candidate’s campaign and one representative from each party allowed to observe (25 P.S. §3146.8(1.1)).

While the official process cannot begin until Election Day, county boards of elections collect and record mail-in ballots that have been returned. According to a Department of State guidance, once receiving mail-in ballots, officials stamp the date of when a ballot was received and scan the “correspondence ID barcode” that is found on the outer envelope. Each issued mail-in ballot has its own unique correspondence ID, and Pennsylvania’s Statewide Uniform Registry of Electors (SURE) will not accept the same ID twice. The SURE system also records when a ballot is received and if a ballot has been cancelled. All ballots are then stored in a secure location until they can be pre-canvassed and canvassed on Election Day.

During the pre-canvassing and canvassing process, there are several reasons why ballots may be set aside and not counted. Voters using a Pennsylvania mail-in ballot are instructed to place their ballots into two envelopes. The ballot goes first into the smaller envelope, labeled “Official Election Ballot,” which is designed to hide the identity and party of the voter (25 P.S. §1304-D). If the ballot arrives without this “secrecy envelope,” it is set aside and not counted, as ordered by a recent Pennsylvania Supreme Court ruling. Furthermore, if there is any indication of the voter’s identity or party on the “Official Election Ballot” envelope, the ballot is set aside and not counted (25 P.S. §3146.8(4)(ii)). The voter is also instructed to place the smaller envelope with the ballot into the larger envelope that has the

voter's declaration and the voter's county, district, and signature ([25 P.S. §1304-D](#)). Any deceased voters' ballots are set aside, as well as any ballots that are [blank](#).

The county board of election then checks the name on the ballot envelope against the "Registered Absentee and Mail-in Voters File" and/or the "Military Veterans and Emergency Civilians Absentee Voters File" through the [SURE](#) system to verify that the individual is registered and has a right to vote ([25 P.S. §3146.8\(3\)](#)). During this time, a member of the board may challenge a ballot "on the basis that the applicant is not qualified to vote," according to a recent Department of State [directive](#), but cannot challenge the ballot "based on signature analysis." If not challenged or discarded, the inner envelope is opened and the ballot is tallied ([25 P.S. §3146.8](#)). Ballots that have been challenged are set aside for a hearing ([25 P.S. §3146.8\(5\)](#)) and the challenge is recorded in the [SURE](#) system.

Although individual county boards of election in Pennsylvania have much discretion when it comes to counting methods and use of technology, they generally apply a similar process. For each mail-in ballot, a clerk scans the outer envelope, opens and scans the inner "secrecy" envelope, then finally opens the inner envelope and scans the ballot into a county tabulation system. For example, in [Montgomery County](#), clerks scan outer envelopes as well as the ballots within and have invested in "ballot extraction devices and high-density scanners." [Philadelphia County](#) has also invested in "high-speed scanners and other equipment." The outer envelope must be opened [without](#) being damaged, as they must be stored for two years after the election ([25 P.S. § 3150.17](#)). County vote tabulation systems cannot be "connected to or permitted on internet-facing networks," according to the [Department of State](#).

There have been and are still several ongoing negotiations, lawsuits, and bills that may affect vote-by-mail procedures in Pennsylvania. One such [lawsuit](#) concerns the recent opening of several [satellite election offices](#) in Philadelphia. [Satellite election offices](#) allow voters to register to vote, request a mail-in ballot, and return it, all in a single visit. The Trump campaign [sued](#) Philadelphia, alleging that the absence of poll watchers at these satellite election offices violates election law. A federal judge [rejected](#) the lawsuit and the campaign [appealed](#) the decision, but their appeal was also [rejected](#). There was also a Republican-sponsored [resolution](#) in the state legislature that made it out of committee, seeking to create a "Select Committee on Election Integrity," but Republicans in the legislature later [cancelled](#) the session to vote on the resolution and halted plans to pursue the committee further. In addition, there are [ongoing negotiations](#) in the legislature to consider passing a law that would allow counties to start processing mail-in ballots earlier. For example, one [proposal](#) would allow for a 21-day [pre-canvass](#) period for mail-in ballots prior to Election Day. Another [bill](#) that has been introduced in the House would allow for a 10-day pre-canvass period. No new legislation appears likely to pass before the election.

Tabulating the Vote

Pennsylvania's tabulation of in-person ballots begins in each district when polls close at 8:00 PM on election night ([25 P.S. §3031.13](#)). In districts with paper ballots or ballot cards, officials announce the vote totals, compare them with a voting checklist to check for any discrepancies, and input the tabulation into a voting system, if they have one ([25 P.S. §3031.13\(g\)](#)). If the district tabulates votes through a voting system directly, then the automated tabulation process begins at the close of polls ([25 P.S. §3031.13\(f\)](#)). For the most part, voting machines tabulate the district's votes, printing out a summary of the returns for each individual machine. Pennsylvania recently required all counties to upgrade their voting systems to a new safety standard, outlined by the Department of State, that mandates "voter-verifiable paper records" be printed from each machine, so that there is a paper trail for votes.

Individual districts are responsible for delivering a copy of their vote counts to their counties. When the district has a system to tabulate votes, two copies of the results in the form of "district total cards" (i.e., memory cards) and "reporting forms" are made ([25 P.S. §3031.13\(b\)\(f\)](#)). These are sealed in envelopes; one copy stays in the district and one is physically delivered to the county board of election ([25 P.S. §3031.13\(f\)\(g\)](#)). In Allegheny County, however, the physical returns are transferred from precincts to regional centers and then electronically relayed to the county, according to a January 2019 [study](#) by the Blue Ribbon Commission at the University of Pittsburgh. Returns, supplies, and provisional ballots must be delivered to county offices by 2:00 AM the day after the election ([25 P.S. §3031.13\(j\)](#)). It is also the responsibility of districts to publicly post the results at the district polling place ([25 P.S. §3031.13\(f\)](#)).

County boards are responsible for aggregating district results, through tabulation machines at a "central tabulation center" ([25 P.S. §3031.14](#)). Although counties [have](#) a wide array of election voting and management systems that they can use to tabulate and create records of the vote, all such systems must satisfy a statewide set of security [requirements](#). In addition to aggregating results, county boards canvass and count write-in ballots and provisional ballots.

There are a few cases when a voter may cast a provisional ballot. If an individual comes to the polls and their identity is not verifiable, and their proof of identity and right to vote is challenged (perhaps because their name does not appear on the list of registered electors), then they may cast a provisional ballot ([25 P.S. §3050](#)). In addition, if an individual requested a mail-in ballot but goes to vote at the polls on Election Day and does not bring their mail-in ballot to be discarded, then their vote is cast as a provisional [ballot](#). (Polling locations' lists of voters will [include](#) those that have applied but not returned a mail-in ballot.) Within seven days of the election, county boards of election evaluate the

provisional ballots and make a determination on each provisional ballot's validity ([25 P.S. §3050.4](#)). If the board determines the ballot is valid, it will be included in the tabulation ([25 P.S. §3050.4\(5\)\(i\)](#)). Otherwise, the ballot is securely stored, and, within seven days of the challenge, a hearing will be held where the voter can object to the decision ([25 P.S. §3050](#)).

Reporting the Vote

The regulation of election night reporting comes mostly from Department of State directives. Under [25 P.S. § 3031.14\(e\)](#), counties “*may* unofficially report the progress of the count.” The Department of State (DOS) points voters to a designated public [website](#) where county boards of election submit uncertified election counts by uploading exported files from their election management system to the [SURE](#) portal. (Please note, this website and other DOS sites have had outages as recently as [October](#).) Although most counties directly submit election night returns to the DOS electronically, a few counties report them via fax, and some counties allow the DOS to manually “scrape” election returns from the county’s website (according to a January 2019 [study](#) by the Blue Ribbon Commission at the University of Pittsburgh). This [study](#) further claims that, for counties that submit returns electronically, the computer they use to transmit the results should be completely separated from other computer components connected to the election management system. Some counties also have their own public-facing web portals where they announce uncertified vote counts, on election night and in the days following. Allegheny County, for example, has a designated [website](#) for election night reporting.

A recent [directive](#) from the Department of State lays out additional guidelines for how and when to submit returns, given the potential for a drawn-out tabulation period. The Department of State has [directed](#) county boards to label counting groups and report them to the Department of State as falling under one of three categories: “Election Day, Mail (combination of absentee and mail-in ballots), Provisional.” County boards of election [must](#) submit the following counts on election night to the Department of State, along with a daily updated version, after election night: “1) a precinct-level results file; 2) a county-level summary report from the EMS system; and 3) a precinct-level summary report from the EMS system.” This same [directive](#) asks counties to submit updated reports at the close of polls, daily as the canvassing process continues, during certification, and when they submit the final results per county.

Certifying the Vote

County boards of election start the process of canvassing and certifying the vote count at 9:00 AM the third day after the election ([25 P.S. §3154\(a\)](#)). This process has been outlined by a DOS [checklist](#). [First](#), the commissioners retrieve and check the total registration number of each district and

verify that it aligns with the elector lists and voting machine lists. If the commissioners find discrepancies, then this triggers an investigation by the return board ([25 P.S. § 3154\(b\)](#)), which, barring special circumstances, consists of two or more judges from the court of common pleas ([25 P.S. § 3153\(b\)](#)). The number of ballots, extra ballots, spoiled ballots, and absentee ballots are then verified and discrepancies accounted for ([25 P.S. § 3154\(c\)](#)). Finally, the paper ballot returns for each district (from district totals cards) are read out loud and checked for discrepancies (on the general returns sheet) ([25 P.S. § 3154\(d\)](#)). If a district used machines, the individual machines registration number and returns are read out loud and checked for discrepancies. Lastly, the board conducts “a statistical recount of a random sample of ballots” ([25 P.S. § 3031.17](#)), which must be a manual recount of ballots or “e-ballot images contained in the system” (according to a 2011 [directive](#)). Official results, “certified under the seal of the county,” are delivered to the Department of State in [physical form](#).

Wisconsin

Like Michigan and Pennsylvania, Wisconsin is another state that may not be able to announce a winner of its statewide vote on election night due to the volume of absentee ballots. The state cannot begin processing absentee ballots until Election Day, and cannot begin counting votes [until the polls close](#) at 8:00 PM CT. Wisconsin’s [decentralized](#) election administration system allows municipalities significant flexibility in choosing procedures, including how mail-in ballots are processed. This flexibility may result in some localities being able to report results sooner than others. At 28 days before the 2016 general election, 172,760 absentee ballots had been mailed out; 28 days out from the November 2020 election, the state has issued 1,252,602 absentee ballots (a 625% increase).

Wisconsin law [provides](#) the basic structure for processing, counting, and certifying election results. Ballots cannot be opened and counted [until](#) Election Day. After ballots are returned, clerks must verify that the ballot envelopes have both voter and witness signatures and that address requirements have been met. Clerks then contact voters who did not meet requirements, open the ballot envelopes, feed ballots through voting machines and, finally, tally the votes. Tallying the votes can only occur [after](#) the close of the polls.

The steps in processing mail-in ballots can be time-consuming, as officials verify signatures, open envelopes, and flatten ballots crumpled in transit to feed into voting machines. These procedures may create a [backlog](#) of millions of votes, which could delay reporting of results. A key step of this process, checking for voter and witness signatures, may hold significant influence over the final election result. Thousands of mail-in ballots have been rejected for missing signatures in past elections: in the April 2020 primary election, [14,042](#) ballots were rejected for missing signatures (out of [23,196](#) total

rejected absentee ballots). For comparison, the 2016 election in Wisconsin was decided by only [22,748](#) votes.

- [Video: How Wisconsin Counts Absentee Ballots](#) - Wisconsin Elections Commission

Processing Mail-In Ballots

Absentee ballots in Wisconsin are carefully collected and securely stored until Election Day, when they are [transported](#) to local polling places, or in some communities, a central counting facility. [Most localities](#) in Wisconsin, including most rural areas and small municipalities, as well as some larger cities such as Madison, intermingle mail-in ballots and in-person ballots at the polling places. Ballot processing and counting procedures at polling place locations are defined by [Wis. Stat. 6.88](#). All ballots are counted together so that, when the precinct count is released, it contains both in-person and mail-in ballots.

Other localities, such as [Milwaukee](#), Kenosha, Waukesha, and Janesville, process mail-in ballots at a central counting location, following state law [Wis. Stat. § 7.52](#). [Thirty-nine municipalities](#) this year will process mail-in ballots at a “Central Count Absentee Ballot site.” A municipal board of absentee ballot canvassers, [composed of](#) the municipal clerk (or a qualified elector designated by the clerk) and two other qualified electors of the municipality appointed by the clerk, will convene at a public location any time after the opening of the polls and before 10:00 PM on Election Day to count the absentee ballots for the municipality. The board of absentee ballot canvassers will follow the [same procedures](#) as those used at the polling place when processing, counting, and securing absentee ballots. Just like at regular polling places, [election observers](#) from political parties and other organizations may observe the processing and counting of absentee ballots at these designated sites. (Wis. Stat. [§ 7.41](#).)

Wisconsin waits until [after the polls open](#) on Election Day to begin processing mail-in ballots. Processing is the act of verifying the identity of the voter who returned the mail-in ballot. There are multiple steps to processing a ballot before counting begins. The election inspectors [must ensure that](#):

1. The voter’s certification has been properly executed,
2. the voter is a qualified elector of the ward or election district,
3. the voter has not yet voted in the election,
4. the ballot has been endorsed by the issuing clerk,
5. The voter has enclosed proof of residence, if required under Wis. Stat. [§ 6.34](#), and such proof matches the name and address on file (if not enclosed, the ballot is marked as provisional), and

6. the voter's name does not appear on the poll list as ineligible to vote by reason of a felony conviction. If the voter does have a felony conviction, the inspectors will challenge the ballot as provided in Wis. Stat. § [6.92](#).

If the election inspector or board of absentee ballot canvassers find no reason to reject the absentee ballot, they mark the elector's name on a poll list and [deposit](#) the voter's ballot into the proper ballot box. **But inspectors will [reject](#) a ballot if they find one of the following issues:**

1. A certification is insufficient: the ballot envelope has no voter signature, no witness signature, no witness address, both special voting deputies failed to sign, and / or no certification language;
2. the applicant is not a qualified elector in the ward or election district;
3. the ballot envelope is open or has been opened and resealed;
4. the ballot envelope contains more than one ballot of any one kind;
5. the certificate is missing for a military or overseas elector who received an absentee ballot by fax or email; or
6. there is proof that an absentee ballot has been submitted for a voter who has since died.

When an absentee ballot is rejected, an inspector [will](#) endorse the rejected ballot on the back, writing "rejected (giving the reason)." They will then reinsert the rejected ballot into the certificate envelope and securely seal the ballot in the envelope inside an envelope marked for rejected absentee ballots. [The inspectors then](#) endorse the "rejected ballots" envelope with a statement of the ward or election district and date of the election, signed by the chief inspector and one of the inspectors representing each of the two major political parties (or every member of the board of absentee ballot canvassers), and return the envelope to the municipal clerk in the same manner as official ballots voted at the election. Ballots rejected because of issues with certification, such as no voter signature, [may be returned](#) to voters on Election Day to provide them the opportunity to cure the certification defects [before the polls close](#) at 8:00 PM. But notice and cure practices across Wisconsin [vary widely](#). In some counties, election officials make an effort to [call every voter](#) whose ballot does not meet witness requirements and help them fix the ballot. Despite the rule that ballots may not be processed before Election Day, county clerks may [inspect the outside](#) of a mail-in ballot as soon as it is received to notify a voter of a missing signature. In other counties, only a small number of ballots that failed to meet the witness requirements [made it](#) to the eventual count.

Rejection of absentee ballots is a major concern for November. In the past, deficiencies in the absentee ballot's certification form, which requires the signature of the voter and a witness, have been responsible for the [majority of rejections](#). In the April 2020 primary elections, more than [23,000 absentee ballots](#) were invalidated, [14,042](#) due to voters or their witnesses failing to sign the absentee

ballot envelope. Anticipating that these [high rejection rates](#) may cause issues in November, the Wisconsin Elections Commission launched a [public relations campaign](#) to provide better instructions to voters on filling out a ballot, fulfilling the witness requirement, correcting mistakes, and returning the ballot once completed. (See [Healthy Election's Signature Verification Memo](#) for a discussion of Wisconsin ballot rejection rates due to ballot defects, the witness form verification process, ballot cure, and related litigation.)

Absentee ballots must be received by the close of polls on Election Day in order to be counted. This law was recently the [subject of litigation](#) as Democrats have sought a more flexible deadline. On September 21, U.S. District Judge William Conley [ruled](#) that ballots that arrive up to six days after Election Day would count as long as they are postmarked by Election Day; but, on October 8, the 7th Circuit [blocked](#) the extension of Wisconsin absentee ballot deadline, and the U.S. Supreme Court [agreed](#) on October 26 to uphold the Wisconsin law. As a result, voters must still get their ballots to the polls by Election Day to be counted. However, at the [39 municipalities](#) including Milwaukee and Green Bay that count absentee ballots at a central location, voters should [check](#) with their municipal clerk about where to return their ballots on Election Day.

Tabulating the Vote

In Wisconsin, no ballots may be counted until the polls close. This late start to the counting process has elicited [concerns](#) that the results of the 2020 election will likely not be known for days. Yet the Wisconsin Elections Commission [maintains](#) that the system of counting votes on Election Night and canvassing votes in the following days is designed to ensure an “accurate, honest, and transparent tabulation and reporting of the people’s will at the ballot box, as well as to detect actual fraud.”

Wisconsin legislators have debated allowing votes to be tabulated before polls close but have not enacted any changes. The Assembly approved a [bill](#) in 2019 that would have allowed some in-person votes cast early to be counted sooner, but that bill died in the Wisconsin Senate. A Senate committee heard testimony earlier this year on a [bill](#) that would have allowed clerks to count absentee ballots early, but it, too, failed to pass. Therefore, for the November 2020 election, the counting of votes will be done after the polls close at [8:00 PM](#) on Election Day

Vote counting at polling places is performed by the election inspectors, otherwise known as “[poll workers](#).” Each polling place generally has [seven](#) inspectors, though more can be appointed. The governing body of a municipality may also appoint [tabulators](#) to assist election inspectors in the counting of votes after polls close.

Immediately after the polls close, the inspectors proceed to canvass all votes received at the polling place. The canvass, whether conducted at the polling place or at a central counting location, must continue without adjournment until the canvass of all ballots cast and received on or before Election Day is completed and the results are reported (Wis. Stat. [7.51\(1\)](#)).

The process of counting ballots is detailed in the [Wisconsin Election Day Manual](#) (2020), which includes detailed procedures for hand-counted paper ballots, optical scan ballots, and Direct Recording Electronic Voting Equipment (DRE). For example, the hand-counted ballot procedure follows [these basic steps](#) (“Counting Ballots”):

1. If there are multiple ballot boxes, open boxes one at a time.
2. Count the ballots in each box (without examining them) to determine the total number.
3. Determine if the number of ballots is equal to the number of voters. (If not, and there is no alternative reason for the ballot overage, election officials [randomly withdraw](#) the number of ballots equal to the excess number of ballots and set those aside.)
4. Count and record the votes on two separate Tally Sheets. Reconcile the tally sheets when the counting for each office is complete.
5. Announce the results of the votes cast at the polling place and prepare all election materials for delivery to the municipal clerk.

[Wisconsin law does not specify the manner for actually counting paper ballots.](#) The Election Commission [recommends](#) a process in which one election official reads each ballot, a second official observes, and two other election officials mark the votes on tally sheets, which are then compared for accuracy at the end of counting. However, [most](#) Wisconsin polling locations use optical scanning devices or voting machines for tabulating ballots, which record the votes and drop the marked ballots into a locked container. [Verified Voting](#) offers a detailed breakdown of election ballot-marking and tabulation equipment by county.

For locations that tabulate votes using Direct Recording Electronic Voting Equipment (DRE), the counting process is straightforward. [All votes, including write-in votes, are automatically tabulated by the DRE equipment.](#) After the polls close, election workers [print out a tape](#) which lists the tabulated vote totals. Inspectors [then](#) record the serial numbers on the security seals and secure a copy of the results (plus the memory cards, unless they remain sealed in the machines) in a sealed envelope bearing the signatures of the chief election inspector and two additional inspectors across the seal. The machine-produced record of the total votes cast for each candidate is [presumed correct](#), unless an error in the record is clearly apparent or unless a candidate at the election requests that the machine be viewed. Voting machines provide [three](#) redundancies: the original ballots in their secured container, the

print-out tape from the machine, and the electronic memory device from the machine. Wisconsin creates a paper record of every vote that is cast, no matter what kind of ballot or equipment voters use.

In addition to following the steps for the Direct Recording Electronic (DRE) equipment, locations which use optical scanning devices must be aware of extra procedures to tabulate ballots that were not legible to the machine. For example, a ballot rejected by the machine must be examined by two election officials from different political parties to determine the cause for rejection. The officials can then make a duplicate ballot to correct the problem (see “Remaking Ballots” in the [WEC Election Day Manual](#)). For some machines, write-in ballots must be tabulated by hand, which may require an edit to the printed results if, for instance, an elector fills in an oval next to a candidate’s name and also writes in a candidate for that office, but fails to complete that oval. Write-in votes, even if the arrow/oval is not completed, [are counted instead](#) of the vote for the candidate on the ballot if the write-in is a registered candidate. Therefore, the returns may need to be amended to reflect the correct number of votes.

The Wisconsin Elections Commission (WEC) offers [extensive instructions](#) for counting irregular ballots in accordance with Wis. Stat. § [7.50\(2\)](#). When a voter has marked a ballot in a way that does not clearly indicate their voting objective, such as when an elector has overvoted an office on the ballot, the election inspectors must attempt to determine the voter’s intention. All inspectors must be part of the determination process, and the majority must agree that the voter’s intention can or cannot be determined. Rules for counting [write-in votes](#) also prioritize voter intent—for example, an irregular write-in vote may be counted if the intent of the voter can be determined, even if a name is misspelled. A ballot that is damaged, overvoted, or otherwise unclear as to voter intent is called a “[defective](#)” ballot. Whenever a ballot is found to be defective, cast by a [challenged elector](#), or rejected (e.g. for missing a signature), the ballot must be identified with a number and set aside, and a notation about the rejected ballot must be made on the [Inspectors’ Statement](#).

Reporting the Vote

Wisconsin law specifies the process of election night reporting. After tallying the votes, election officials [announce](#) the results of the votes cast at the polling places and prepare all election materials for delivery to the municipal clerk. On election night, election inspectors [must](#) report the returns, by ward or returning unit, to the county clerk no later than two hours after the votes are tabulated (Wis. Stat. § [7.51\(4\)\(c\)](#)). Wisconsin [does not](#) have an official statewide Election Night reporting system. According to Wis. Stat. § [7.60\(1\)](#), the clerks must post all returns, by ward or reporting unit, on an internet site maintained by the county no later than two hours after receiving the returns on election night. Some counties (such as [Adams County](#)) post results via Google Drive folders linked from their county website, while others report results directly on their websites. The Election Commission of Wisconsin

advises voters to refer to this [list](#) of Wisconsin County election websites on election night to find unofficial results from Wisconsin's 72 County Clerks or [to look for](#) reporting by local news outlets, which aggregate and report statewide results.

Certifying the Vote

Vote totals in Wisconsin are [triple-checked](#). Election results from municipalities are not official until they have been double-checked by the county and [certified](#) by the bipartisan Wisconsin Elections Commission. The tally from election inspectors on election night is the *unofficial* election result; the official results of the elections are [not finalized until later](#) (see "Post Election Activities"). To certify the vote, each official board of canvassers must meet to complete the official canvass of their respective offices (at the municipal, county, state, or other level). The canvass statement is the [official](#) determination of the outcome of the election. The election is not complete and no recount can be requested until the canvass has been completed (Wis. Stats. §§ [7.53\(4\)](#), [9.01\(1\)\(a\)](#)).

The canvass for the presidential race takes place at the [county level](#). Immediately following the county canvass, the county clerk [delivers](#) to the Elections Commission the certified statements from the county board of canvassers, with the election returns recorded by ward. County canvassers must certify their results to the Wisconsin Election Commission ("WEC") by [November 17, 2020](#), 14 days after the election (Wis. Stat. § 7.60(5)). The WEC must certify the statewide results by [December 1, 2020](#) (Wis. Stat. § 7.70(3)(a)).

Candidates and electors may petition for a [recount](#) until 5:00 PM on the third business day following certification by the official board of canvassers. As soon as this deadline for filing a petition for a recount has passed, the municipal clerk issues a [Certificate of Election](#) to each person elected to any municipal office. When a valid petition for a recount is filed, the municipal clerk must wait to issue the certificate of election for the office in question until the recount has been completed and the time allowed for filing an appeal has passed or, if appealed, until the appeal is decided (Wis. Stat. § [7.53\(4\)](#)). Wisconsin recount laws are [summarized in detail](#) by the Citizens for Election Integrity Minnesota.

Conclusion

Counting the vote, especially mail-in votes, is a complex process even in the most efficient states. [The 2020 expansion of vote-by-mail among states with little prior experience counting large numbers of absentee ballots will inevitably cause counting to take longer than in previous elections.](#) In those states where processing and counting begins on Election Day, it will take longer than usual to count ballots and report results. Depending on how close the election is and whether certain

late-processing battleground states (Michigan, Pennsylvania, and Wisconsin) will be dispositive for the outcome, the presidential race may take several days before the winner is known with a high degree of certainty. However, because of the decentralized administration and reporting system in these states, election night may produce valuable information from the local level that can signal which way the political winds are blowing. If the election night results are indeterminate, however, we should expect absentee ballots to be a fertile source for conflict and litigation in the post-election period.

Appendix

Key Links:

[Actually, We Will Know a Lot on Election Night](#) - Nate Persily and Charles Stewart III, Wall Street Journal

[How to Survive Election Night](#) - Nate Persily and Charles Stewart III, Slate

[Counting the Vote During the 2020 Election](#) - Bipartisan Policy Center

[How Quickly Will Your Absentee Vote Be Counted? A State-by-State Timeline](#) - New York Times

[State Recount Laws Searchable Database](#) - Citizens for Election Integrity Minnesota

[Verified Voting \(Election equipment used in each county\)](#)

Exhibit 2.



Login (<https://www.ncsl.org/login.aspx?returnurl=%2fresearch%2felections-and-campaigns%2fall-mail-elections635457869.aspx>)

Create Account (https://www.ncsl.org/fon_registration.aspx?returnurl=https%3a%2f%2fwww.ncsl.org%2fresearch%2felections-and-campaigns%2fall-mail-elections635457869.aspx)

Contact (</aboutus/ncslservice/ncsl-contact.aspx>) | Help (</aboutus/ncslservice/ncsl-website-guide.aspx>)

ABOUT US ▾ (/ABOUTUS.ASPX) LEGISLATORS & STAFF ▾ (/LEGISLATORS-STAFF.ASPX) RESEARCH ▾ (/RESEARCH.ASPX)

MEETINGS & TRAINING ▾ (/MEETINGS-TRAINING.ASPX) NCSL IN D.C. ▾ (/NCSL-IN-DC.ASPX) NEWS ▾ (/BOOKSTORE/STATE-LEGISLATURES-MAGAZINE.ASPX)



GENERAL INFORMATION

Download free PDF
(/LinkClick.aspx?
fileticket=-
ltr5LyV7IM%3d&tabid=285

Order LegisBrief
Subscription
(<http://comm.ncsl.org/OnlineStore/tabid/54/Default.aspx?ProductId=2196>)

NCSL Bookstore
(<http://comm.ncsl.org/OnlineStore/tabid/54/Default.aspx>)

Legisbriefs Home
Page
(<http://comm.ncsl.org/Default.aspx?tabid=177&class=LegisBrief>)

NCSL CONTACTS AND RESOURCE

Wendy Underhill
| 303-856-1379
(mailto:wendy.underhill@ncsl.org)

Michael D.
Hernandez | 303-
856-1474
(mailto:michael.hernandez@ncsl.org)

Katy Owens Hubler
| 303-856-1656
(mailto:katy.hubler@ncsl.org)

NCSL's Vote-by-Mail
Web page
(<http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx>)

All-Mail Elections

By Michael D. Hernandez | Vol . 22, No. 35 / September 2014



Did You Know?

- At least 22 states allow certain elections to be conducted entirely by mail.
- Legislators introduced 42 bills in 2013-2014 that related to vote-by-mail elections.
- Although supporters of vote-by-mail emphasize its apparent convenience for voters, critics have cited concerns about its reliance on the U.S. Postal Service.

Voters more often are casting their ballots from home as states have increasingly allowed all mail elections to take the place of traditional precinct polling place voting. Voters in Colorado, Oregon and Washington need never visit a traditional neighborhood polling place. Instead, these three states administer all elections entirely through the mail. This trend has been quietly growing and is prompting legislators to consider whether all-mail elections are a good fit for their state or community.

For such elections, all registered voters in a jurisdiction receive a mailed ballot. A participating voter marks the ballot and places it inside a secrecy envelope or protective sleeve, which then is placed inside a separate envelope. This envelope is signed by the voter as an affidavit to his or her identity and returned to an election office. Occasionally, voters in other states have used the same voting method that previously was afforded only to qualified absentee voters. At least 22 states have provisions that allow certain elections to be conducted entirely by mail.

Pros and Cons. Supporters of all-mail elections say allowing a person to cast a vote from the comfort of his or her home boosts convenience and helps people avoid wait times at polling places. The voter also can take as much time as needed to thoroughly examine the ballot. Elections administrators say all-mail elections reduce the costs of recruiting and training workers for polling places; it also frees them from the sometimes challenging task of finding a suitable polling location. Some rural jurisdictions appreciate the flexibility all-mail elections provide local governments. They no longer need to devote resources to the infrastructure and personnel required to administer an election at traditional in-person voting precincts. These vote-by-mail elections have slightly increased turnout for special elections and some municipal elections that often fail to garner attention from voters and the media.

2021 LEGISLATIVE SESSION

Welcome back Rely on NCSL

Contact your NCSL State Liaison for personal assistance.

(<https://www.ncsl.org/aboutus/ncsls-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncsls-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncsls-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncsls-state-liaisons-map.aspx>)

ADDITIONAL RESOURCES

Changing the Way Colorado Votes: A Study of Selected Reforms,"Colorado Secretary of State, 2011
(<http://www.ucdenver.edu/academics/colleges/SPA/Documents/Election%20Reform%20Study%202011-11.pdf>)

Oregon's Vote-by-Mail Procedures Manual,"
(<http://sos.oregon.gov/elections/Pages/Vote-by-Mail-Procedures-Manual.aspx>)

Elections and Campaigns

All Documents

(<https://www.ncsl.org/searchresults/issearch/false/kwId/458.aspx>)

Initiative and Referendum
(<https://www.ncsl.org/searchresults/issearch/false/kwId/462.aspx>)

Election Administration
(<https://www.ncsl.org/searchresults/issearch/false/kwId/463.aspx>)

StateVote Election Results and Analysis
(<https://www.ncsl.org/searchresults/issearch/false/kwId/463.aspx>)

Campaign Finance
(<https://www.ncsl.org/searchresults/issearch/false/kwId/460.aspx>)

Opponents of all-mail elections say the voting method weakens the traditional civic experience of voting with neighbors at a local school, church or community polling place. They maintain that vote-by-mail's cost savings are largely nullified by the expenses to print and mail ballots to each registered voter in a jurisdiction. Although all-mail elections increase turnout in special and small elections, they have not successfully encouraged voter participation in larger general elections. Finally, opponents say all-mail elections do not provide the level of security and voter confidence inherent in polling place voting. They contend that ballots can be lost at any stage of the vote-by-mail process, that such a system relies on an already strained U.S. Postal Service, and that voters outside a polling place can be more easily coerced into selecting candidates and measures they do not support.

State Action

Colorado, Oregon and Washington are the only states that administer all elections entirely by mail. Other states permit vote-by-mail in certain elections, such as special elections, municipal elections, when a candidate is proposed, or at the discretion of the county clerk. The kinds of jurisdictions that use all-mail elections vary. Some states have relied on the voting method to address a shortfall in elections resources. In Idaho, for example, a county with a precinct that has no more than 125 registered voters can use all-mail elections. Hawaii, which has some of the lowest turnout rates in the country, has sought to increase voter participation by allowing jurisdictions to use vote-by-mail for local and special elections.

Some jurisdictions that have moved to all-mail elections have noted significant savings because they no longer need to spend money for recruitment, training and pay for polling place workers. When Montana considered an expansion of vote-by-mail to administer all elections in 2011, the state's association of clerks and recorders estimated the move would save taxpayers \$2 million each election cycle. In Colorado, a county survey estimated that costs in 2010 would have amounted to \$1.05 less per registered voter, a savings of about 19 percent.

However, some of the savings from administering an election entirely by mail are offset by an increase in postage costs for each registered voter to be mailed a ballot. Since Americans are highly mobile, the task of ensuring voter registration rolls are updated becomes even more essential in an all-mail election.

Security. The secure delivery of ballots is a key concern about all-mail elections. Academic research has found absentee ballots can be lost in transit for a variety of reasons, including ballots requested but not received, ballots transmitted but not returned for counting, and ballots returned for counting but rejected. This loss of votes could affect a close election.

Some jurisdictions have offered voters the use of ballot-tracking systems that allow a person to follow where his or her ballot is in the delivery and counting process. In addition, some jurisdictions provide ballot drop boxes to address voters' concerns that ballots might not be returned in time to be counted.

PDF Version (</LinkClick.aspx?fileticket=-ltr5LyV7IM%3d&tabid=28575&portalid=1>)

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)
(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)



We are the nation's most respected bipartisan organization providing states support, ideas,

Members Resources

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)

(<https://www.ncsl.org/aboutus/ncslservice/ncsl-state-liaisons-map.aspx>)

Policy & Research Resources

- Bill Information Service (<https://www.ncsl.org/aboutus/ncslservice/bill-information-services-overview.aspx>)
- Legislative Websites (<https://www.ncsl.org/aboutus/ncslservice/state-legislative-websites>)

Meeting Resources

- Calendar (<https://www.ncsl.org/aboutus/ncslservice/meetings-training/ncsl-meetings-calendar.aspx>)
- Online Registration (<https://www.ncsl.org/aboutus/ncslservice/meetings-training/ncsl-meetings-calendar.aspx>)

Press Room

Denver

7700 East First Place
Denver, CO 80230
Tel: 303-364-7700 | Fax: 303-364-7800

Washington

440 North Capitol Street, N.W., Suite 515
Washington, D.C. 20001
Tel: 202-624-5400 | Fax: 202-737-1069

connections and a strong voice on Capitol Hill.


- map.aspx)Get Involved With NCSL (/legislators-staff.aspx)
- Jobs Clearinghouse (/legislators-staff/legislative-staff/jobs-clearinghouse-service.aspx)
- Legislative Careers (/legislators-staff/legislative-staff/legislative-staff-coordinating-committee/legislative-careers.aspx)
- NCSL Staff Directories (/aboutus/ncslservice/ncsl-staff-directories-and-online-requests.aspx)
- Staff Directories (/aboutus/ncslservice/staff-directory-search-form.aspx)
- Terms and Conditions (/aboutus/ncslservice/ncsl-website-terms-and-conditions.aspx)


- directory.aspx)
- NCSL Bookstore (/bookstore.aspx)
- State Legislatures Magazine (/bookstore/state-legislatures-magazine.aspx)
- Accessibility Support
- Tel: 1-800-659-2656 or 711 (tel:18006592656)
- Accessibility Support (/aboutus/ncslservice/ncsl-accessibility-help.aspx)
- Accessibility Policy (/aboutus/ncslservice/ncsl-accessibility-policy.aspx)


- Media Contact (/press-room.aspx)
- NCSL in the News (/press-room.aspx)
- Press Releases (/press-room.aspx)


Go 28575


Go

 (https://www.facebook.com/pages/Denver-CO/National-Conference-of-State-Legislatures/89855016270)

 (https://twitter.com/NCSLorg)

 (https://www.youtube.com/user/NCSLorg)

 (https://www.linkedin.com/company/national-conference-of-state-legislatures)

 (https://www.instagram.com/ncslorg/)

This website uses cookies to analyze traffic and for other purposes. You consent to the use of cookies if you use this website.

Continue

Exhibit 3.

ADVERTISEMENT



Click to copy

RELATED TOPICS

- Election 2020
- Joe Biden
- Donald Trump
- Politics
- U.S. News
- AP Top News
- Elections
- Voting
- William Barr
- Politics AP

AP

Disputing Trump, Barr says no widesprea...

Top Stories Topics Video Listen

Disputing Trump, Barr says no widespread election fraud

By MICHAEL BALSAMO December 1, 2020



ADVERTISEMENT

WASHINGTON (AP) — Disputing President Donald Trump’s persistent, baseless claims, Attorney General William Barr declared Tuesday the U.S.

Trending on AP News

NOT REAL NEWS: A look at what didn’t happen last week

Biden attends Mass at DC church where

Justice Department has uncovered no evidence of widespread voter fraud that could change the outcome of the 2020 election.

Barr’s comments, in an interview with the The Associated Press, contradict the concerted effort by Trump, his boss, to subvert the results of last month’s voting and block President-elect Joe Biden from taking his place in the White House.

Barr told the AP that U.S. attorneys and FBI agents have been working to follow up specific complaints and information they’ve received, but “to date, we have not seen fraud on a scale that could have effected a different outcome in the election.”

The comments, which drew immediate criticism from Trump attorneys, were especially notable coming from Barr, who has been one of the president’s most ardent allies. Before the election, he had repeatedly raised the notion that mail-in voting could be especially vulnerable to fraud during the coronavirus pandemic as Americans feared going to polls and instead chose to vote by mail.

More to Trump’s liking, Barr revealed in the AP interview that in October he had appointed U.S. Attorney John Durham as a special counsel, giving the prosecutor the authority to continue to investigate the origins of the Trump-Russia probe after Biden takes over and making it difficult to fire him. Biden hasn’t said what he might do with the investigation, and his transition team didn’t comment Tuesday.

Trump has long railed against the investigation into whether his 2016 campaign was coordinating with Russia, but he and Republican allies had hoped the results would be delivered before

he worshipped as VP

Legislator who questioned Black hygiene to lead health panel

by Taboola

ADVERTISEMENT

"One Percenter's" Powerful New Message: Things Are About to Get Ugly

Click

AP

China pushes fringe theories about virus

the 2020 election and would help sway voters. So far, there has been only one criminal case, a guilty plea from a former FBI lawyer to a single false statement charge.

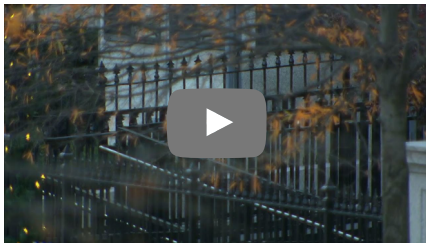
RELATED STORIES:

- [Republicans call for resignation of Wisconsin election chair](#)
- [Trump files lawsuit challenging Wisconsin election results](#)
- [Wisconsin, Arizona certify Biden wins in presidential vote](#)

Under federal regulations, a special counsel can be fired only by the attorney general and for specific reasons such as misconduct, dereliction of duty or conflict of interest. An attorney general must document such reasons in writing.

Barr went to the White House Tuesday for a previously scheduled meeting that lasted about three hours.

Trump didn't directly comment on the attorney general's remarks on the election. But his personal attorney Rudy Giuliani and his political campaign issued a scathing statement claiming that, "with all due respect to the Attorney General, there hasn't been any semblance" of an investigation into the president's complaints.



Attorney General William Barr said Tuesday the Justice Department has not uncovered evidence of widespread voter fraud that would change the outcome of the 2020 presidential election. (Dec. 1)

Other [administration officials who have come out forcefully](#) against Trump's allegations of voter-fraud evidence have been fired. But it's not clear whether Barr might suffer the same fate. He

maintains a lofty position with Trump, and despite their differences the two see eye-to-eye on quite a lot.

Still, Senate Democratic leader Chuck Schumer quipped: “I guess he’s the next one to be fired.”

Last month, Barr issued a directive to U.S. attorneys across the country allowing them to pursue any “substantial allegations” of [voting irregularities](#) before the 2020 presidential election was certified, despite no evidence at that time of widespread fraud.

That memorandum gave prosecutors the ability to go around longstanding Justice Department policy that normally would prohibit such overt actions before the election was certified. Soon after it was issued, the department’s top elections crime official announced he would step aside from that position because of the memo.

The Trump campaign team led by Giuliani has been [alleging a widespread conspiracy](#) by Democrats to dump millions of illegal votes into the system with no evidence. They have filed multiple lawsuits in battleground states alleging that partisan poll watchers didn’t have a clear enough view at polling sites in some locations and therefore something illegal must have happened. The claims have been repeatedly dismissed including by Republican judges who have ruled the suits lacked evidence.

But local Republicans in some battleground states have followed Trump in making unsupported claims, [prompting grave concerns](#) over potential damage to American democracy.

Trump himself continues to rail against the election in tweets and in interviews

though his own administration has said the 2020 election was the most secure ever. He recently allowed his administration to begin the transition over to Biden, but he still refuses to admit he lost.

The issues they've have pointed to are typical in every election: Problems with signatures, secrecy envelopes and postal marks on mail-in ballots, as well as the potential for a small number of ballots miscast or lost.

But they've gone further. Attorney Sidney Powell has spun fictional tales of election systems flipping votes, German servers storing U.S. voting information and election software created in Venezuela "at the direction of Hugo Chavez," – the late Venezuelan president who died in 2013. Powell has since been removed from the legal team after an interview she gave where she threatened to "blow up" Georgia with a "biblical" court filing.

Barr didn't name Powell specifically but said: "There's been one assertion that would be systemic fraud and that would be the claim that machines were programmed essentially to skew the election results. And the DHS and DOJ have looked into that, and so far, we haven't seen anything to substantiate that."

In the campaign statement, Giuliani claimed there was "ample evidence of illegal voting in at least six states, which they have not examined."

Full Coverage: [Election 2020](#)

"We have many witnesses swearing under oath they saw crimes being committed in connection with voter fraud. As far as we know, not a single one has been interviewed by the DOJ. The Justice Department also hasn't audited any voting machines or used

their subpoena powers to determine the truth,” he said.

However, Barr said earlier that people were confusing the use of the federal criminal justice system with allegations that should be made in civil lawsuits. He said a remedy for many complaints would be a top-down audit by state or local officials, not the U.S. Justice Department.

“There’s a growing tendency to use the criminal justice system as sort of a default fix-all,” he said, but first there must be a basis to believe there is a crime to investigate.

“Most claims of fraud are very particularized to a particular set of circumstances or actors or conduct. ... And those have been run down; they are being run down,” Barr said. “Some have been broad and potentially cover a few thousand votes. They have been followed up on.”

Associated Press Writers Lisa Mascaró and Eric Tucker contributed to this report.

ADVERTISEMENT





PAID FOR BY VISIT UTAH



Utah's Best Hot Springs: Let Mother Earth Warm Your Soul

The fun goes way beyond sitting and soaking.



NOT REAL NEWS: A look at what...

A roundup of some of the most ...

January 22, 2021

Ad Content

This Is Who Really Makes Costco's...

Promoted:
MoneyWise.com

The Dead Giveaway That Tells You When...

Promoted: Capital One
Shopping

Millennials Don't Like These Brands...

Promoted:
MoneyWise.com

Texas: Say Bye To Expensive Solar Panels If You Li...

Promoted:
EnergyBillCruncher

Biden attends Mass at DC...

WASHINGTON
(AP) — President...

yesterday

Legislator who questioned Blac...

COLUMBUS, Ohio
(AP) — A ...

January 22, 2021

Ad Content

5 Stocks For Retiring Early

Promoted: The Motley Fool

Deepest Hole On Earth Permanently Sealed After Finding 2 Billion Year Old Fossil

Famous Economist: How Dollar Crash Will Unfold

Promoted: Stancherry Research

Trump shuns 'ex- presidents club' ...

WASHINGTON
(AP) — It's a club...

January 23, 2021

AP source: Biden to drop Trump's...

WASHINGTON
(AP) — President...

2 hours ago

ADVERTISEMENT



 Click to copy

AP NEWS

- Top Stories
- Video
- Contact Us

DOWNLOAD AP NEWS

Connect with the definitive source for global and local news



MORE FROM AP

- [ap.org](#)
- [AP Insights](#)
- [AP Definitive Source](#)
- [AP Images Spotlight](#)
- [AP Explore](#)
- [AP Books](#)

FOLLOW AP

THE ASSOCIATED PRESS
[About](#) [Contact](#) [Customer Support](#) [Careers](#) [Terms & Conditions](#) [Privacy](#)
All contents © copyright 2021 The Associated Press. All rights reserved.

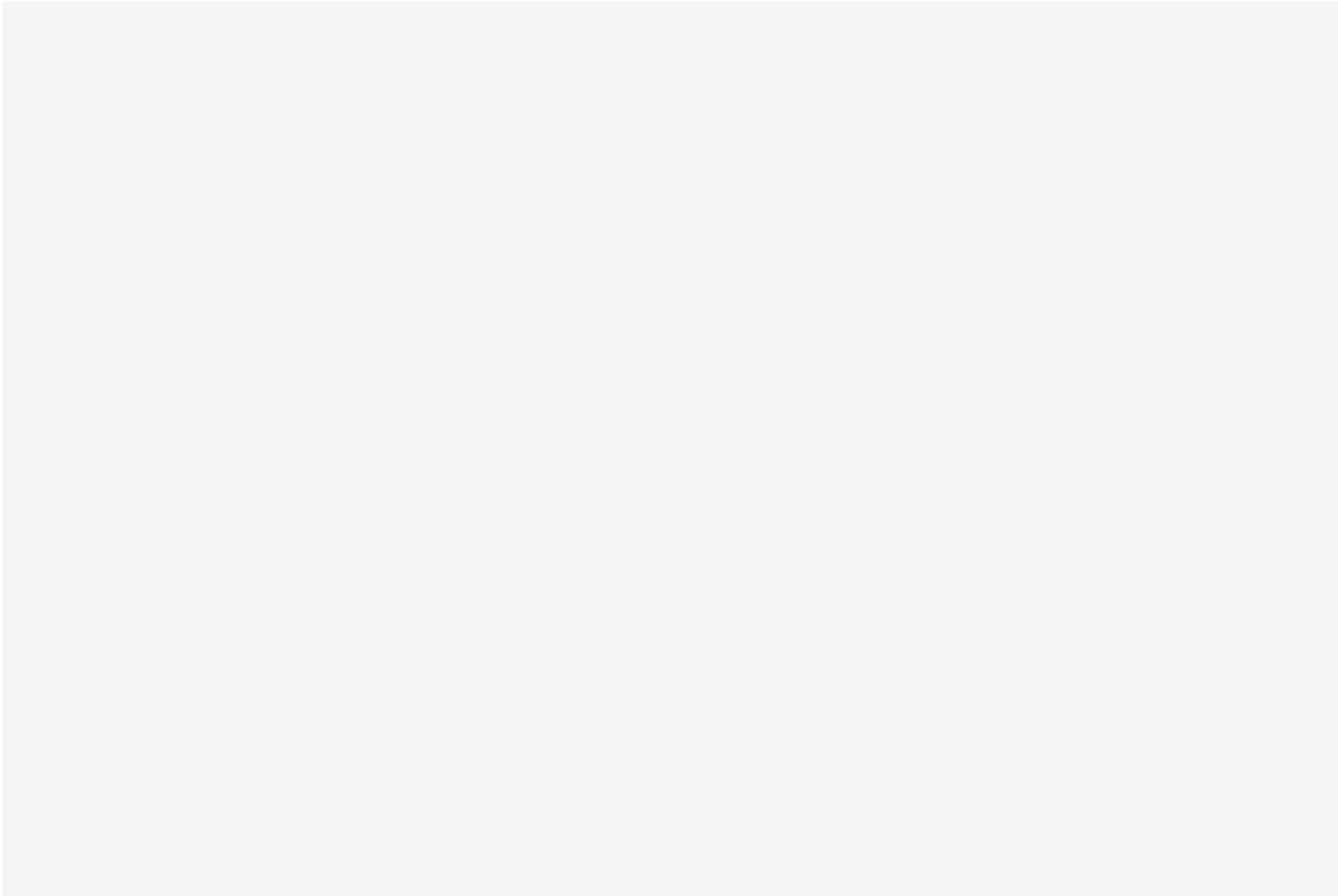


Exhibit 4.

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/221411287>

Methods of Information Hiding and Detection in File Systems

Conference Paper · January 2010

DOI: 10.1109/SADFE.2010.17 · Source: DBLP

CITATIONS

7

READS

6,626

3 authors, including:



[Jeremy Davis](#)

Mississippi State University

4 PUBLICATIONS 19 CITATIONS

[SEE PROFILE](#)



[David Anthony Dampier](#)

Marshall University

56 PUBLICATIONS 269 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Smartphone Forensics [View project](#)

Methods of Information Hiding and Detection in File Systems

Jeremy Davis, Joe MacLean, David Dampier
Department of Computer Science and Engineering
Mississippi State University
Mississippi State, MS

jed81@msstate.edu jm795@msstate.edu dad6@msstate.edu

Abstract—Multiple methods of information hiding can be used by criminals to conceal incriminating data. The FAT and NTFS file systems are the most commonly used file systems in operating systems today, and therefore are the most exploited. Most methods of information hiding can be detected using forensic tool kits designed specifically for cyber crime investigators. The purpose of this paper is to explore various methods of information hiding in the FAT and NTFS file systems)

Keywords- Digital forensics, information hiding, file system, FAT, NTFS, slack space, file slack, disk slack, bad cluster, free space, steganography, forensic toolkit, deleted file, hidden file, directory entries, alternate data streams, master file table, hidden partition, computer forensics analysis

I. INTRODUCTION

Information hiding, accomplished by exploiting a computer's file system and various other operating system characteristics, can take on many forms. In many cases, information hiding is a intentional activity that an individual employs to store away sensitive information in an attempt to make it invisible to everyone else. However, there are some exceptions, such as digital watermarking, that are used for appropriate purposes. Some common methods of information hiding include: hidden files, deleted files, hidden partitions, alternate data streams, steganography, and slack space hiding. There are many computer forensics tool kits available that allow a user to detect multiple types of information hiding. Taking a more in depth look to how these tool kits detect the types of information hiding mentioned gives a deeper understanding of how the information hiding was accomplished.

The most widely used file systems for Windows operating systems are the file allocation table (FAT) file systems and the new technologies file system (NTFS). These file systems both perform the same basic tasks, but for the purposes of information hiding, their subtle differences change the ways that some methods of information hiding are accomplished. Thus, a brief overview of each file system, along with a small discussion of their differences is warranted and shall be presented prior to the discussion of the various methods of information hiding.

II. FAT FILE SYSTEMS

The FAT or File Allocation Table file system is one of the simplest file systems used today. Its simplicity is mainly due to its compatibility with multiple operating systems and its small number of data structures [1]. Because of this, many cross-platform storage devices, such as thumb drives, use FAT file systems to avoid complications when running the device on other machines with different operating systems. However, as Carrier [1] points out, the simplicity has lead to many modifications used to give the system new capabilities. Also, FAT does not follow the five-category model laid out by Carrier [1]. This is mainly due to its low number of data structures that perform duties for more than one category. This makes it easier to analyze the FAT file system in terms of its data structures as apposed to breaking it down into the five categories of file system data. The FAT file system uses two primary data structures, the file allocation table and directory entries [1].

III. NTFS FILE SYSTEMS

The New Technologies File System (NTFS) was designed by Microsoft and is the default file system for Microsoft Windows NT, Windows 2000, Windows Server, and Windows XP [1]. NTFS is also the default file system for Windows Vista and Windows 7.

The master file table (MFT) is the primary data structure and it contains information about all files and directories of the file system [1]. Each entry in the MFT contains attributes that describe the file. These attributes are denoted by a name beginning with a '\$'. One important aspect of the NTFS file system is that everything is treated as a file, even the MFT.

The NTFS file system is a more complex and advanced file system. Its introduction was supposed to provide a more reliable and secure file system than FAT [1]. However, NTFS file systems are still susceptible to virtually all of the same methods of information hiding that the FAT file systems are.

IV. REASONS FOR INFORMATION HIDING

Not all information hiding is done for criminal purposes. Hidden partitions can be used to place a system recovery partition on the disk. Also, hidden partitions can be used when you need to install multiple legacy operating systems that do not usually work well when installed simultaneously [3]. Steganography can be used for digital watermarking in an attempt to prevent copyright infringement. Alternate Data Streams (ADS) can be used to allow a file to contain additional property information. For the purposes of this paper, however, let us discuss the methods of information hiding from a perspective of both the criminal and the investigator.

V. INFORMATION HIDING METHODS

A. Hidden Files and Folders

Possibly the most simple method of information hiding a person could use is hidden files or folders. All Microsoft Windows operating systems allow a user to set properties for a file or folder. Taking this into consideration, a criminal could simply store whatever information they choose in a file or a folder of files and mark the file or folder as hidden from the Windows file properties dialog box. Since this is the simplest method of information hiding, it is also the most easily detectable method of information hiding. In order to detect hidden files or folders in a Windows operating system, an investigator simply has to enable the viewing of hidden files and folders from the folder view submenu. This almost eliminates the method of hiding data in hidden files and folders for criminal purposes.

B. Deleted Files

According to Davis et. al., "one of the most common tasks requested in any investigation is to find and recover the files that have been deleted from the system. This will often be a prime indicator of what the suspect is trying to hide if you find mass deletions before your imaging occurred" [2].

Multiple factors are taken into account when designing file systems. For the final user of the system, more often than not they are concerned with the speed and throughput of the system as opposed to the security. Taking this into consideration, the designer of the operating system has a couple of options when implementing the way the file system will handle deleted files. First, the operating system can overwrite the data on disk and remove it completely, or the operating system can mark the file as unallocated in the FAT or MFT. Since the second option is much less time intensive, the operating system designer usually chooses this option.

By choosing this design option, the operating system designer opens up the possibility of hiding information in deleted files. The only caveat to hiding information by deleting files is that the person must make sure that the clusters the files once resided in will not be overwritten once deleted. Due to the increasing capacity of disks, and the design option of allowing deleted files to still reside on disk but not in the MFT or FAT, the possibility of a deleted file being overwritten is small. This is due to the file allocation algorithms used by most modern operating systems. Operating systems tend to allocate files in a linear fashion [2]. This causes new file allocation to occur toward the end of the disk. As a result, deleted files toward the beginning of the disk have a better chance of not being overwritten. This will be especially true for smaller deleted files since the file system will attempt to allocate larger files sequentially. The large files cannot be completely stored in the clusters of the deleted file, so the file will be stored further down in memory.

Recovering deleted files using modern forensic tool kits requires the same process in both FAT and NTFS file systems. These tool kits examine the allocation status of the file and will inform the user whether or not the file has been deleted or unallocated. Also, these tool kits will allow the investigator to examine the deleted files [2].

C. Hidden/Deleted Partitions

As with files, it is also possible to mark a partition as hidden or deleted. Hidden partitions, although possible, are almost useless when hiding information for criminal purposes. This is because most common file systems have standardized ways of dealing with hidden partitions. Every operating system as well as any partition manager will recognize these partitions even though they are hidden, and some Linux distributions mount these hidden partitions by default. The method for marking a partition as hidden manually is rather straightforward. If a user flips the fifth most least significant bit in the partition ID, the partition is hidden [3].

Deleted partitions are a little more useful for information hiding. All operating systems make use of a master boot record (MBR) which is located in the first block on the drive and contains a pointer to a boot loader that either allows the user to choose from multiple operating systems installed or loads an operating system from a partition on a drive. All file systems are accessed through the MBR. The MBR also contains a partition table for each partition that has information about the partition on the drive. It is possible for a user to delete the partition table, or entries in the partition table, using various utilities freely available [2]. The deleted partitions still remain on the disk just as deleted files/folders do, so it may be possible to recover or reconstruct these partitions using most computer forensic tool kits.

Recovering deleted partitions is a bit more complex, but it follows along the same lines as recovering deleted files. For the FAT file system, a deleted partition can be recovered by locating the first and last sector of a deleted partition. Forensic tool kits allow you to search for the first and last sectors of an object, and since the first and last sectors of a FAT partition are standard, an investigator can simply perform a search for these items to recover the deleted FAT partition [2]. The process is the same for recovering deleted NTFS partitions. The only difference is the starting sector of the NTFS partition contains a different value [2].

D. Alternate Data Streams

Alternate Data Streams (ADS) are a method of information hiding that is only possible on NTFS file systems. The previously mentioned attributes associated with each file on a NTFS system gives way to ADS. Each file has an associated \$DATA attribute that describes the content of the file. More than one \$DATA attribute that is associated with a file is an ADS [1]. These additional data attributes will not be shown when the contents of a directory are listed, so the hidden \$DATA attributes can be used by individuals to hide information [1]. An ADS becomes invisible to someone using a tool such as Windows Explorer to view a file. Thus, the existence of an ADS is undetectable to average users that are not using a utility that can be used to view the structure of a file [2]. Furthermore, the size of the file (when viewed through a tool such as Windows Explorer) does not increase, no matter how large the alternate data is. Therefore, it is easy to see how a suspect could use this method to hide sensitive information rather secretly.

The following example will show how easy it is to create an ADS using the Windows command line tool. Assume that the user has a file named "new.txt," then in the command line the user enters the command "echo Hidden Data>new.txt:secret.txt." This command creates a new \$DATA attribute for "new.txt" named "secret.txt" with the string "Hidden Data." Following this, the user enters the command "notepad new.txt:secret.txt." to open the "secret.txt" \$DATA attribute for "new.txt." When notepad opens, the user will now see "Hidden Data" in the file, as opposed to opening "new.txt" normally where they would see whatever information is contained in the actual file [5]. Luckily for the investigator, most modern tool kits can detect and reveal ADS.

Almost all of the modern forensic tool kits provide the capability to display ADS. Given that an NTFS image is provided, these tool kits will detect and display the information hidden in an ADS to the investigator. The investigator simply has to be aware that ADS may exist on a NTFS image and that ADS may contain hidden information [2].

E. Slack Space

Slack space refers to the remaining data from a previously allocated file in a cluster that has been overwritten on disk. Since a cluster is fixed in size, any newly allocated data that did not fill the entire cluster would still contain data from the last allocated file. Searching a disk using a non-forensic tool would cause a user to miss all of the data contained in the slack space. It is possible, if a user can figure out how to delete files in such a way that new files are allocated to the position of the file they wish to hide, to use slack space for criminal information hiding purposes [2]. However, all modern computer forensic tool kits capture the entire disk when imaging a drive and therefore show all data that remained in slack space. So any information hidden in the slack space will be revealed once the image is examined in such a tool kit. As such, a discussion of how to detect disk slack space hiding is not warranted because it is revealed with the disk image acquisition.

F. File Slack Space Hiding

Since the file system has some basic size for a cluster, there is frequently space left over in allocated clusters at the end of files. Shu-fen et al [6] describe a method for hiding files in this slack space found at the end of other files. This process is similar to hiding files in free space; however, the file will have to be divided into varying size segments based on the slack space sizes available. To find slack space, it is necessary to analyze the directory entries. This data structure will contain the size of the files in the system. "If the file size is a non-integer multiple of the size of the cluster, we can calculate the size of the remaining space in the final cluster" [6]. Again, the cluster numbers and size of the data stored must be stored and encrypted in order to restore the file. As such, there will be no directory entry for the hidden file because of the manual storage of file segments. Again, the locations of the file segments could be decrypted if the configuration file can be found. Also, the hidden file contents will easily be seen following the end of the file.

G. Bad Clusters

In their paper, Shu-fen and others [6] describe a method for hiding files in “bad” clusters. The basic technique relies on the file allocation table and its manipulation. The file is split up into segments based on the size of the clusters used by the FAT file system. The segments are then placed in unallocated spaces as identified by the file allocation table. This process mimics the normal allocation done by the file system except that there is no entry for the file in the directory entries. As each segment of the file is placed in unallocated clusters, that cluster is marked as “bad” in the file allocation table. This can be done directly because the start position of the file system can be found based on the type of FAT [6]. To keep track of the clusters that compose the hidden file, each “bad” cluster is recorded in a configuration file and encrypted. This technique tries to completely hide a file in unallocated clusters manually, by avoiding the default behavior of file allocation. By doing this, there will be no directory entry for the file, and the file clusters can be manually marked as “bad” in the file allocation table. To recover the file, the used cluster numbers must be decrypted and used to read the segments of the file in memory [6]. Of course, this method has its drawbacks. An encrypted list of sectors must be kept in order to reconstruct the file. If this list is stored in the same file system, there is the possibility it will be found and decrypted. An even easier way to uncover the presence of such a file would be to analyze the file using some sort of forensic tool kit. A forensic tool kit is capable of identifying bad clusters and allows the user to view the contents if the cluster is indeed not bad.

H. Steganography

Steganography means “concealed writing” and refers to many types of information hiding. For the purposes of this paper, let us consider image steganography. This is perhaps the most complex and useful information hiding technique. Also, it is the most difficult to detect and uncover. An image file is usually large in size compared to a text or short audio file, thus image files can be used to plant steganography that will go undetected to a typical user [4]. According to Kessler, “the most common steganography method in audio and image files employs some type of least significant bit substitution or overwriting” [4]. If a user wanted to hide a short text file or something similar in an image file, changing the least significant bit changes very little in the image and it is not very likely that a human could detect the alterations. This is a very simple implementation of image steganography. Most steganography creation tools use some sort of algorithm to randomize which bits are actually changed in the image. This factor is what makes steganography detection so difficult [4].

Detecting steganography is a very complex task. One approach to detect steganography is to inspect the structure of the medium to detect oddities. A human eye may not be able to detect image manipulation in this way, but perhaps a software tool would. Least significant bit alterations cause multiple duplicate colors. Sometimes these duplicate color patterns can give some insight into what algorithm was used when hiding the data. Furthermore, longer hidden messages will alter the carrier image more severely, so the suspect will have to choose a large enough image so that the hidden information will still go undetected. Kessler also mentions that this type of statistical analysis is commonly employed to detect hidden messages when the hidden information to be detected is unknown [4]. Finally, Kessler points out that recovering the hidden information is much more complex than simply detecting the hidden information. When recovering the hidden information, the investigator must have some sort of insight into the message length and perhaps some knowledge of the algorithm used [4].

VI. CONCLUSIONS

Information hiding is a factor in each computer forensics investigation. There are several methods of information hiding that a suspect can use to conceal incriminating evidence. Most modern tool kits provide methods for detecting, recovering, and viewing most all types of information hiding. Thus, the investigator's job is made much easier with the advent of these tool kits. However, as these tool kits make detecting the common methods of information hiding more trivial, it is plausible that new and more innovative ways of information hiding will be developed to circumvent the current methods and thwart the tool kits' capabilities.

REFERENCES

- [1] B. Carrier, “File System Forensic Analysis,” Addison-Wesley, Upper Saddle River, NJ, 2005.
- [2] C. Davis, A. Phillip, and D. Cowen, “Hacking Exposed: Computer Forensics Secrets & Solutions,” McGraw-Hill, Emeryville, CA, 2005.
- [3] “Hide Data in Hidden Partitions,” <http://blog.crowdway.com/2009/04/15/hide-data-in-hidden-partitions/> (current 8 November 2009).
- [4] G. C. Kessler, “An Overview of Steganography for the Computer Forensics Examiner,” *Forensic Science Communications*, vol. 6 no. 3, July 2004. Available online: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
- [5] “Practical Guide to Alternative Data Streams in NTFS,” <http://www.irongeek.com/i.php?page=security/altlds> (current 8 November 2009).
- [6] L. Shu-fen, P. Sheng, H. Xing-yan, and T. Lu, “File Hiding Based on FAT File System,” *Proceedings IEEE International Symposium on IT in Medicine & Education*, Ji’nan, China, vol. 1, 2009, pp. 1198-1201.

Exhibit 5.



23
NOV

By EC-Council / Fundamental, Speed Reading

6 ANTI-FORENSIC TECHNIQUES THAT EVERY CYBER INVESTIGATOR

EC-Council | Blog



SUBSCRIBE TO EC-

EC-COUNCIL NEWS SPEED READING CYBER RESEARCH

MEMBERS' FEEDBACK ABOUT

anization to stealing crucial data, cybercriminals can

form a wide range of nefarious activities. In some cases, these perpetrators try to cover their tracks by deleting browser history, cache memory, and even cookies. But with an **upward trend**, it is now much more convenient for cyber attackers to use already programmed software and tools to alter their digital footprints. Technically, these tools are designed to hide, remove, and eventually hinder cyber forensic analysis. With the use of anti-forensic techniques, it becomes **exhausting to retrieve evidence during a computer investigation**.

Cybercriminals use many ways to hide information and their digital footprints. For instance, altering the header of a file can deceive people. Changing the header from .jpg to .mp3 will give the impression of an audio file, but the system will still treat it as an image file.

Similarly, an **investigator** focused on a particular file format can skip over important evidence. Under another method, perpetrators can use slack space, i.e., unused space of a file, to hide sensitive sections of a file. Dividing a file into smaller sections and hiding the information in the slack space, makes the data retrieval and data assembly challenging.

The internet has a vast number of **anti-forensic techniques** to conceal the digital activities of an individual. Some of these techniques are basic, while some require sound technical knowledge. The advanced techniques are deliberately used by the **black hat** community to hamper a **cyber investigation**.

Name*

Email*

Write for Us

- ☐ By signing up, you agree to EC-Council using your data in accordance with our Privacy Policy (<https://www.eccouncil.org/statement/>) & Terms of Use (<https://www.eccouncil.org/of-use/>). We use your data to personalize and improve your experience as an user and provide the services you request from us. You can change your preferences or unsubscribe any time by editing your profile on your Member Dashboard or by clicking

Fascinating Anti-Forensic Techniques to Cover Digital Footprints

1. Encryption

*Under **encryption**, the data is converted into an unreadable format (“encrypted data” or “ciphertext”) using a pair of keys.*

The primary motive of encryption is to prevent confidential files or data from unauthorized access. The encrypted data can be deciphered only by using the paired-up key. This is one of the traditional methods to protect data.

Under modern cryptography methods, Data Encryption Standard (DES), Advanced Encryption Standard (AES), are a few of the popular techniques. They use symmetric as well as asymmetric encryption.

Difference between symmetric and asymmetric algorithms?

Symmetric algorithms use a single key to encrypt and decrypt data, while asymmetric algorithms use two separate keys for both the processes.

2. Steganography

Steganography is the act of concealing data in plain sight.

Most often, data is exchanged via an image. In this type of technique, a section of the image is altered so that it

CATEGORIES

- **EC-COUNCIL NEWS**
- **SPEED READING**
 - **FUNDAMENTAL**
 - **INTERMEDIATE**
 - **ADVANCED**
- **EC-COUNCIL DOSSIER**
- **MEMBERS FEEDBACK**

is not identifiable easily. The processed file looks ordinary and can go unnoticed. In the modern-day, the message is concealed using microdots and invisible ink. There is another form, linguistic steganography, where the message is hidden in a natural context. Steganography allows messages and even huge files to be hidden in pictures, text, audio, and video files.

It is challenging to identify a steganography-attack, but repetitive patterns can reveal the secret message to the investigator. With that, the professionals can also use advanced tools to spot hidden data.

3. Tunneling

This method uses encapsulation to allow private communications to be exchanged over a public network.

The data packets will flow from public networks, thus generating no suspicion. One of the common ways is to use a **Virtual Private Network (VPN)**, which encrypts the data for security reasons.

To eliminate such attacks, organizations must continuously monitor their encrypted network connections.

4. Onion Routing

The process of sending messages which are encrypted in layers, denoting layers of an onion, is referred to as onion routing.

LATEST ARTICLES

**WHAT IS
CYBER THREAT
INTELLIGENCE?
ALL YOU NEED
TO KNOW**

22 Jan 2021

**A DAY IN THE
LIFE OF A
SECURITY
OPERATIONS
ANALYST**

22 Jan 2021

**ALVIN ONG,
CHIEF
INFORMATION
OFFICER AT
NANYANG
TECHNOLOGICA
TALKS ABOUT
BECOMING A
CERTIFIED
CHIEF
INFORMATION
SECURITY**

The data packet goes through several networking nodes where every layer of encryption gets peeled off. With the stripping of the final layer, the message gets closer to reach its destination. The message remains anonymous to the entire message delivery chain except the nodes placed after the source and before the destination.

One of the best practices to fight against onion routing is to use reverse routing. This elimination process is time-consuming but can be used to defeat onion routing.

5. Obfuscation

A technique that makes a message difficult to understand because of its ambiguous language is known as obfuscation.

This method uses jargon and ingroup phrases to communicate. It could be intentional and unintentional. The primary objective of obfuscation is to reduce the risk of exposure. It can be done by altering the signature or fingerprint of malicious code.

Deobfuscation is the same as countering onion routing. Removing layers exposes clean and readable code.

6. Spoofing

The act of disguising communication to gain access to unauthorized systems or data.

Spoofing can be performed through emails, phone

**OFFICER
(CCISO)**

21 Jan 2021

Tweets by @ECCOUNCIL

EC-COUNCIL
@ECCOUNCIL
And the countdown begins...
Our compelling roundtable on Effective Security Incident Handling is all set to take place on Jan 28!

Reserve your spot now to receive actionable insights and learnings - bit.ly/3i4ZQVA#cybersecurity
[#informationsecurity](#)
[#security](#)



1h

EC-COUNCIL
@ECCOUNCIL
What does web application security

[Embed](#)

[View on Twitter](#)

calls, and websites. Two most common ways of spoofing are –

- **IP Spoofing** – Under IP spoofing, perpetrators use a different IP address to hide their system's IP address for initiating malicious activities. Generally, this type of spoofing intends to carry out a **distributed denial of service (DDoS)**. It can be performed either manually or by the use of tools.
- **MAC Spoofing** – MAC addresses usually cannot be changed, but with technical skills, it is not impossible. With MAC spoofing, cyber attackers use fake MAC addresses. This is one of the difficult spoofing methods to counter.

Other types of spoofing include ARP spoofing, DNS spoofing, email spoofing, and many more.

Forensic investigators have many **tools and techniques** to identify spoofing, such as examining email headers in the case of email spoofing or investigating wireless access point activities in case of MAC spoofing, and likewise.

Many of these topics are covered under the **Computer Hacking Forensic Investigator (CHFI)**. The program will give you an in-depth understanding of **digital forensics**. Being a hands-on program, its virtual labs mimic the real-world challenges, offering the best learning experience. The vast coverage of CHFI includes database forensics, cloud forensics, operating system forensics, network forensics, mobile forensics, and many

others.

Related Articles

José Sequeira Martins,
Founder & GM at
SCORPIONSHIELD
Talks about his
Cybersecurity journey
with EC-Council Role


Nancy Castillo,
Information Analysis
Specialist in the
National Banking and
Securities
Commission, Speaks
about the EC-Council
CEH Course

Alvin Ong, Chief
Information Officer at
Nanyang
Technological, Talks
about becoming a
Certified Chief
Information Security
Officer (CCISO)


Hassan Abdul Mohsen,
Talks about Becoming
a Certified ethical
hacker

2 Comments

Sort by Oldest




Add a comment...

 **Fae Ghott**

Great read! reccomend this to anyone looking to get into cybersecurity.

Like · Reply · 47w

 **Bhupendra Timilsena**

great understanding about the anti-forensics tools

Like · Reply · 16w

Facebook Comments Plugin

< Don't leave personal data on devices any longer in use – You could be hacked

Local Governments: Ransomware Attack's Hottest Target >

ABOUT POST AUTHOR

EC-Council



©2020 EC-Council

[Partner With Us](#) | [Terms of Use](#) | [Privacy Statement](#) | [Sitemap](#)

Exhibit 6.

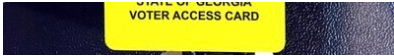
WEATHER ALERTS / Severe Thunderstorm Warning: **Borden**

NATIONAL

Judge blasts Georgia officials' handling of election system



NEWS VIDEO WEATHER SPORTS TV SCHEDULE ABOUT US CONTESTS

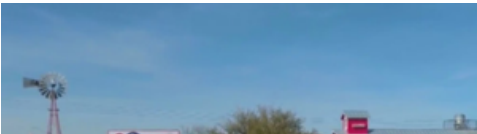


FILE – This May 22, 2018, file photo, shows a voter access card inserted in a reader during voting in the Georgia primary in Kennesaw, Ga. A federal judge has ordered Georgia to stop using its outdated voting machines after 2019. U.S. District Judge Amy Totenberg on Thursday, Aug. 15, 2019, issued the order after voting integrity advocates and individual voters asked her to order the state to immediately switch to hand-marked paper ballots. (AP Photo/Mike Stewart, File)

DON'T MISS

by: **KATE BRUMBACK, Associated Press**
Posted: **Aug 17, 2019 / 07:53 AM CDT** / Updated: **Aug 17, 2019 / 10:56 AM CDT**

This is an archived article and the information in the article may be outdated. Please look at



the time stamp on the story to see when it was last updated.

ATLANTA (AP) — Georgia election officials have for years ignored, downplayed and failed to address serious problems with the state's election management system and voting machines, a federal judge said in a scathing order this week.

U.S. District Judge Amy Totenberg said those problems place a burden on citizens' rights to cast a vote and have it reliably counted. She called Georgia's voting system "antiquated, seriously flawed, and vulnerable to failure, breach, contamination, and attack."

Despite those findings, Totenberg ruled Thursday that Georgia voters will use that same election system this fall because of concerns about the state's capacity to make an interim switch while also implementing a new system .

Plaintiffs in a lawsuit challenging Georgia's system had asked Totenberg to order an immediate switch to hand-marked paper ballots for special and municipal elections this fall. But she declined, citing worries about the state's capacity to manage an interim switch while also implementing a new system that is supposed to be in place for the March 24 presidential primaries.

"(T)he totality of evidence in this case reveals that the Secretary of State's efforts in monitoring the security of its voting systems have been lax at best — a clear indication that Georgia's computerized election system is vulnerable in actual use," Totenberg wrote in a 153-page ruling that devotes considerable space to chronicling those shortcomings.

Here are some of the concerns Totenberg identified:

LACKLUSTER RESPONSE TO A SECURITY LAPSE

Security experts in 2017 disclosed a gaping hole exposing personal data for 6.7 million Georgia voters, as well as passwords used by county officials to access election-staging files. That lapse at the Center for Election Systems at Kennesaw State University, which managed the system for the secretary of state, still wasn't fixed six



Be Our Change – Legendary Barn Door

[Be Our Change](#) / 2 days ago

Odessa neighborhood upset over car vandalisms

[News](#) / 4 days ago

Permian Producers Are Optimistic About Keystone XL Cancellation

[Energy Report](#) / 2 days ago

Jane Doe identified in 54-year- old Pecos cold case

[Local News](#) / 5 days ago

Safe-2-Save Competition

[News](#) / 1 week ago

[More Don't Miss](#) →

months after it was first reported to election authorities.

The relevant servers were wiped soon after the lawsuit was filed. Totenberg said officials' assertions that the servers "were simply 'repurposed ' and not intentionally destroyed or wiped is flatly not credible."

Election officials have refused to "fully acknowledge or remedy these circumstances and their broader ramifications for the voting system's security and reliability," Totenberg wrote. She also said election officials had shown "inconsistent candor" with her about this and other voting system security issues.

The Center for Elections Systems eventually became part of the secretary of state's office. Michael Barnes, who directed it at Kennesaw State remains in that role. But Barnes "could recall little or what expressly was done" after they received notification of the breach, Totenberg wrote.

PROBLEMATIC FROM THE START

Totenberg cited a brief filed by the Electronic Privacy Information Center that says "almost from their inception" the paperless electronic voting machines Georgia has used since 2002 "have been plagued by warnings that the voting machines are unreliable, insecure, unverifiable."

"(W)hile Georgia election officials have effectively taken no steps to address these deficiencies with its DRE-based system — a litany of other states have abandoned the plagued machines in exchange for a more secure and reliable alternative voting method," Totenberg wrote.

BALLOT BUILDING SECURITY

Barnes testified last month that the state's election management system, which is used to build ballots, is housed on private computers not connected to the internet, saying the system is "air gapped." He also testified that he uses a "lockable" USB drive to transfer files between those computers and internet-connected computers.

Relying on testimony from cybersecurity experts, Totenberg wrote that using a USB drive in that way exposes the data to malware and leaves the entire election system vulnerable to contamination.

The state has a contract with election equipment company Election Systems & Software, which employs three people to design and configure Georgia's databases. They built all the ballots for last November's elections, Barnes testified.

They work from home on computers disconnected from the internet, Barnes testified. But Totenberg noted that Barnes couldn't say what physical security measures they have at their homes and that their computers are "outside the secure facilities that the Secretary of State maintains for ballot building."

RISK ASSESSMENTS AND RESPONSE

Fortalice Solutions, a cybersecurity firm hired by the secretary of state's office to do risk assessments, identified 22 security risks in the networks it examined for an October 2017 report. In a subsequent Nov. 30, 2018, report Fortalice found that just three of those risks had been fixed and another three were in the process of being fixed.

Totenberg wrote that the record includes "scant" evidence of what "targeted remedial measures" state officials took following the November 2018 report.

Totenberg also wrote that the state never asked Fortalice or another expert "to conduct an actual cybersecurity review and analysis" of its election-related systems and databases.

VOTER TROUBLES

Totenberg cited a "mountain of voter testimony showing that these vulnerabilities have a tangible impact" on voters' attempts to cast a ballot and have their vote counted.

The plaintiffs provided statements from 137 Georgia voters, two county poll workers and 15 poll watchers about problems during the November 2018 midterm election. Those included: self-casting

ballots, malfunctioning voting machines, voter selections flipping to another candidate, and electronic pollbooks showing incorrect polling places or addresses for voters.

STATE RESPONSE

In an email to The Associated Press, Tess Hammock, spokeswoman for Secretary of State Brad Raffensperger, said, “These conclusions are silly and unfounded. At the end of the day no judge should be susceptible to political Rhetoric.”

In a subsequent email she added that the secretary of state’s office looks forward to implementing the new system.

Much of what Totenberg mentioned took place while now-Gov. Brian Kemp was secretary of state. Kemp spokeswoman Candice Broce didn’t respond to emails seeking comment.

Lawyers for the state have argued that implementing a new election system resolves the problems of the old system.

State election officials testified that steps were taken to ensure the election management system’s safety when it was transferred from Kennesaw State, and that they had acted to remedy vulnerabilities identified in risk assessments.

During a hearing last month, under questioning by a plaintiffs’ attorney, Barnes said, “I feel confident in Georgia’s voting system, yes.”

Copyright 2021 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

SHARE THIS STORY ►

AROUND THE WEB

 revcontent.





Jackie Kennedy Was a Style Icon - but Her Shoes Revealed What We Long Suspected

Maternity Week



George Gilder Presents Tiny Little Device Set to Boom in 2021

George Gilder With 6



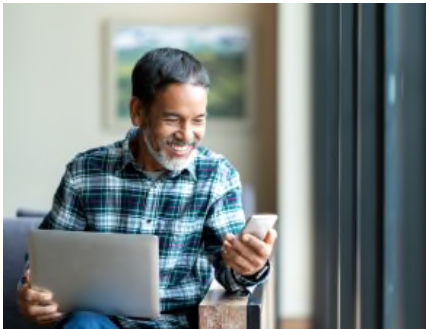
Frisco, These Are The Most Successful Lawyers

Find Attorneys | Sponsored



Federal Program Will Pay Off Your Home If You Live In Texas

Mortgage Benefits



Our Five Free Stock Picks for 2021

The Motley Fool



See Your Personalized Numerology Reading

Numerologist



Do This Immediately if You Have Diabetes (Watch)

healthtoday



Why is This \$47 Monocular Better Than \$3000 Telescopes?

StarScope





Diana's Butler Reveals Why Harry Really Married Meghan

Maternity Week

MORE NATIONAL STORIES



AP Source: Sarah Sanders running for Arkansas governor

by ANDREW DeMILLO, Associated Press / Jan 24, 2021

[Read the Full Article](#) →



Grizzly, 34, confirmed as Yellowstone region's known oldest

Jan 24, 2021

[Read the Full Article](#) →



Chicago teachers vote to teach from home, defying district

by SOPHIA TAREEN, Associated Press / Jan 24, 2021

[Read the Full Article →](#)





FOLLOW US



NEWS APP



WEATHER APP



[News](#) [Video](#) [Weather](#) [Sports](#) [TV Schedule](#) [About Us](#) [Contests](#) [Community](#) [Jobs](#)

[Contact Us](#) / [About Us](#) / [TV Schedule](#) / [NewsNation Now](#) / [KMID: FCC Public File](#) / [KPEJ: FCC Public File](#) / [EEO Public File](#) / [Certification of Compliance Training](#)
[Privacy Policy](#) / [Terms Of Use](#) / [Covers](#) / [VENN.tv Gaming News](#) / [Do Not Sell My Personal Information](#) / [FCC Applications](#) / [Public File Assistance Contact](#)



© 1998 - 2021 Nexstar Inc. | All Rights Reserved.

Exhibit 7.

247SPORTS



LOG IN

JOIN

- News ▾
- Boards ▾
- Football ▾
- FB Rec ▾
- Basketball ▾
- BB Rec ▾
- Podcasts
- More
- Shop

Judge allows GA to reset & wipe Dominion voting machines data

Submit

Reply

Back To Topics

dinkum

Nov 29th, 2020, 6:55 PM

UPDATE– Judge Timothy Batten reversed claim later today.

What??? Judge reversed order based on Defendants' claim that GA Counties control voting machines.

Machines are owned by State & @GaSecofState administers state laws on elections.

Why are GA officials determined to wipe these machines clean be resetting them?

<https://t.co/Oq0edTGfsl>

— Lin Wood (@LLinWood) November 29, 2020



LOCKED TOPIC - NO MORE REPLIES CAN BE POSTED



STICKY NOTE



PREMIUM TOPIC



EXPERT POSTED ON THIS TOPIC



COMMUNITY THREAD



YOU POSTED IN THIS TOPIC

NEW MESSAGES IN TOPICS YOU VIEWED

HOT TOPIC

WARMER TOPIC

WARM TOPIC

COOL TOPIC

By Jim Hoft

Published November 29, 2020

BREAKING: Judge Timothy Batten Issues Order to Freeze All Dominion Machines in Georgia ...UPDATE: Judge Reverses Order Within Hours

<https://www.thegatewaypundit.com/2020/11/breaking-update-judge-timothy-batten-issues-order-freeze-dominion-machines-georgia/>

Georgia court issues, then reverses order to prevent Dominion voting machines being 'wiped'

A Georgia court briefly granted an order to prevent voting machines being wiped on Sunday, before reversing course.

on Sunday, with a federal judge briefly granting, then reversing, an order seeking to prevent voting machines being wiped.

L. Lin Wood is suing Georgia Governor Brian Kemp, Secretary of State Brad Raffensperger and several members of the state election board in an attempt to de-certify the election results and have Donald Trump declared the winner.

Mr Wood has made sweeping allegations of

election fraud and, among other things, had sought an emergency order “that voting machines be seized and impounded immediately for a forensic audit by plaintiffs’ experts”, as he takes aim at voting machine company Dominion.

NED-2208-US Election-In-Article-Banner - 0

The prominent defamation lawyer – who famously represented Richard Jewell, and more recently Covington student Nick Sandmann and Kenosha shooter Kyle Rittenhouse – also requested an order that “no votes received or tabulated by machines that were not certified as required by federal and state law be counted”.

On Sunday, US District Court Judge Timothy Batten granted Mr Wood’s request for a temporary injunction. “Plaintiffs contend that Union County officials have advised that they are going to wipe or reset the voting machines of all data and bring the count back to zero on Monday, November 30,” Judge Batten wrote.

Should Donald Trump concede?

Yes, Joe Biden has the electoral votes required to win

No, he is right to challenge the result

Cast your vote

“To the extent Plaintiffs seek a temporary restraining order to preserve the voting machines in the State of Georgia, and to prevent any wiping of their data, their motion is granted. Defendants are ordered to maintain the status quo and are temporarily

enjoined from wiping or resetting any voting machines until further order of the court.”

Within hours, however, Judge Batten reversed the order after being advised by the defendants that the machines were controlled by the local counties. “Plaintiffs’ request fails because the voting equipment that they seek to impound is in the possession of county election officials,” he wrote.

“Any injunction the court issues would extend only to defendants and those within their control, and plaintiffs have not demonstrated that county election officials are within defendants’ control. Defendants cannot serve as a proxy for local election officials against whom the relief should be sought.”

Judge Batten ordered Georgia officials to “promptly produce to plaintiffs a copy of the contract between the state and Dominion”. The defendants must file a response by 3pm on Wednesday, with an in-person hearing scheduled for Friday at 10am.

A Fulton County employee moves voting machine transporters to be stored at the Fulton County Election Preparation Center on November 4, 2020 in Atlanta, Georgia.

Picture: Jessica McGowan/Getty Images/AFP

A Fulton County employee moves voting machine transporters to be stored at the Fulton County Election Preparation Center on November 4, 2020 in Atlanta, Georgia.

Picture: Jessica McGowan/Getty

Images/AFPSource:AFP

On Twitter, Mr Wood expressed frustration at the ruling. “Machines are owned by (the) state and (the Secretary of State) administers state laws on elections,” he wrote. “Why are Georgia officials determined to wipe these machines clean (by) resetting them?”

It’s the latest setback for Mr Wood – who is working closely with former Trump team lawyer Sidney Powell – in his bid to overturn the election which saw Joe Biden become the first Democrat to win the southern state for the first time in decades.

Mr Biden beat Mr Trump by 12,670 votes, or 0.25 per cent, according to results that were certified by the State of Georgia after a hand recount and “risk-limiting audit”. The President and state Republicans have claimed the process was “meaningless”, and are instead demanding a full audit of absentee ballot signatures.

Mr Wood unsuccessfully attempted to stop the vote being certified, and is now arguing that the restraining order is also needed for the US Senate run-offs on January 5, where the loss of Kelly Loeffler and David Perdue could hand the majority back to Democrats. On Twitter, however, Mr Wood has attacked both of the Republican incumbents, accusing

them of not supporting the President more forcefully. “It makes NO sense that (Ms Loeffler) and (Mr Perdue) are not demanding (Mr Kemp) order special session of (the) Georgia legislature to address fraud,” he tweeted on Sunday. “Same voting machines, same mail ballots, same fraud. (November 3) fraud will be repeated in run-off.”

In addition to seeking to disqualify millions of mail-in votes, Mr Wood has latched onto more nebulous allegations of electronic vote manipulation by Dominion, which the company has repeatedly rejected as **baseless conspiracy theories.**

Last week, Ms Powell filed her own lawsuit in Georgia, alleging election software and hardware produced by Dominion is where the “massive fraud begins”. Georgia purchased Dominion products in July 2019, a year after Texas rejected the system due to its vulnerability to undetected manipulation. Speaking to Fox News last week, Dominion spokesman Michael Steel said the alleged switching of votes from Mr Biden to Mr Trump could not have occurred because it was “physically impossible”.

“Look, when a voter votes on a Dominion machine, they fill out a ballot on a touch screen,” Mr Steel said. “They are given a printed copy which they then give to a local

election official for safekeeping. If any electronic interference had taken place, the tally reported electronically would not match the printed ballots, and in every case where we've looked at – in Georgia, all across the country – the printed ballot, the gold standard in election security, has matched the electronic tally.”

Sounds familiar

Divide familiar into syllables: fa-mil-iar

Or, in Georgia familiar is divided into fa-mi-liar with the accent on the last syllable.

<https://twitter.com/lilinwood/status/1333140968082649088>

↑ 0 ↓ ○○○

Discussion

dinkum

Nov 29th, 2020, 10:51 PM • 174 months •

7,859

<https://www.zerohedge.com/political/judge-blocks-then-unblocks-georgia-wiping-or-resetting-election-machines>

Judge Blocks, Then Unblocks Georgia
From Wiping Or Resetting Election
Machines

Authored by Ivan Pentchoukov and Petr Svab via The Epoch Times,

A federal judge presiding over a major election lawsuit in Georgia on Sunday issued and then reversed an order directing the state to cease and desist wiping or resetting election machines.

“Defendants are ordered to maintain the status quo & are temporarily enjoined from wiping or resetting any voting machines in the State of Georgia until further order of the court,” Judge Timothy Batten wrote in an emergency order issued Nov. 29.

The judge reversed the order not long after, explaining that the defendants are not in possession of the machines.

“Plaintiffs’ request fails because the voting equipment that they seek to impound is in the possession of county election officials. Any injunction the Court issues would extend only to Defendants and those within their control, and Plaintiffs have not demonstrated that county election officials are within Defendants’ control. Defendants cannot serve as a proxy for local election officials against whom the relief should be sought,” the judge wrote.

The change of course by the judge drew a flabbergasted response from Lin Wood, an

attorney associated with the Trump campaign.

“What??? Judge reversed order based on Defendants’ claim that GA Counties control voting machines,” Wood wrote on Twitter, adding that the machines are owned by the state and that the Georgia secretary of state administers elections.

“Why are GA officials determined to wipe these machines clean [by] resetting them?”

The plaintiffs in the lawsuit on Sunday filed an emergency motion which included an affidavit featuring a Nov. 25 message from an election official stating that the ballot-counting machines would be reset to zero on Monday, Nov. 30, before performing a recount.

“The process will begin with an L & A – resetting the machine to ‘zero’ to begin the recount,” the text of the message stated before describing the specifics of the recount process.

The affidavit was written by a GOP poll worker who says he or she addressed concerns about wiping the machines to the election manager.

“Because the plan on Monday is to wipe

the voting machines clean, and start from 0 so that we can recount using those machines, I'm concerned by what I am reading online," the poll worker wrote, according to the affidavit.

"I am seeing lots of notices from lawyers about possibly impounding the machines. Lawyers are now saying that the machines should be confiscated immediately before this happens to protect forensic data. They are saying those machines need to be impounded ASAP. Yikes. Maybe I'm being overly paranoid but let's be sure this is what we're supposed to be doing."

The supervisor responded, "It's what we are supposed to do. It will take a court order to stop this process—so I guess we need to keep watching the news. If we get a court order to stop, we will see it in our SOS information. The issue is, the Atlanta area has already started," the elections manager wrote.

When the poll worker asked if the reset will wipe the forensic info from the machines, the manager said that "Atlanta already did it."

The lawsuit in question is being litigated by Sidney Powell, an attorney who defended former national security adviser Lt. Gen. Michael Flynn. President Donald

Trump pardoned Flynn earlier this week. The Trump campaign has said that Powell is not part of its legal team.

Georgia Republican Party Chairman David Shafer wrote on Twitter after the judge issued the order that election officials in Fulton County were updating the software on voting systems earlier the same day.

“Our Republican recount monitors at the World Congress Center waited today for four hours while Fulton County elections officials ‘updated the software.’ The explanation given to me—‘just the usual Fulton County incompetence’—is completely unacceptable,” Shafer wrote on Twitter.

“It is outrageous that we cannot rely on Fulton County elections officials to do their jobs without unexplained four hour delays, interventions by private attorneys and federal court orders.”

Voting Systems

The lawsuit makes a number of allegations regarding the voting machines and software supplied by Dominion Voting Systems, which is used in Georgia and many other states.

The lawsuit cites an affidavit written by a former electronic intelligence analyst under 305th Military Intelligence Battalion, who testified that the software used by the Dominion machines was accessed by agents of malicious actors, such as China and Iran, “in order to monitor and manipulate elections,” including the 2020 election.

The suit further alleges that the machines are connected to the internet, even though they aren’t supposed to be, and are easily hacked, based on multiple expert declarations. The machines have built-in functions that allow operators to manipulate the results, several experts cited in the lawsuit said.

Dominion has vehemently denied that its machines were used to manipulate vote counts.

“Servers that run Dominion software are located in local election offices, and data never leaves the control of local election officials,” the company’s website states.

“All U.S. voting systems must provide assurance that they work accurately and reliably as intended under federal U.S. EAC and state certifications and testing requirements. Dominion’s voting systems

are certified for the 2020 elections.”



0



ooo

GABUSC

Nov 29th, 2020, 11:49 PM • 231 months •

8,328

I would think the Republicans would welcome wiping them clean.

The party had whined since the Election took place.

Do you really want the same machines the party claims are part of a made up Fraud charge?

GO SC



1



ooo

Metrobank

Nov 30th, 2020, 8:30 AM • 193 months •

15,917

<https://www.dropbox.com/s/7fewfrnbatz0jb7/THIRD%20ORDER%20-%20PEARSON%20v.%20KEMP%2011.29.2020.pdf?dl=0>

Defendants must file an objection by Wednesday. Looks like the forensic examination of the Dominion voting machines is on in Georgia.

↑ 1 ↓ ○○○

TroyKiddv2

Nov 30th, 2020, 10:01 AM • 35 months •

19,313

dinkum said... (original post)UPDATE– Judge Timothy Batten reversed claim later today.What??? Judge reversed order based on Defendants’ claim that GA Counties control voting machi...

show more

Naw. Nothing to see hear. Totally above board. You Republicans just shut up and move on.

↑ 0 ↓ ○○○

dinkum

Dec 1st, 2020, 1:41 PM • 174 months •

7,859

TroyKiddv2 said... (original post)Naw. Nothing to see hear. Totally above board. You Republicans just shut up and move on.

show more

TroyKidd2, spot on!

Democratic Party & GOP Gangland Wars in Atlanta entered a treaty to remove all evidence while judges held up Temporary Restraining Orders.

[https://en.wikipedia.org/wiki/Gangs_in_Georgia_\(U.S._state\)](https://en.wikipedia.org/wiki/Gangs_in_Georgia_(U.S._state))

Gangs in Georgia

<https://www.zerohedge.com/political/powell-dominion-server-removed-fulton-county-while-lawyers-sought-restraining-order>

Powell: Dominion Server Removed From Fulton County While Lawyers Sought Restraining Order

Authored by Ivan Pantchoukov via The Epoch Times, 1Dec20

Attorney Sidney Powell said on Monday that someone had removed a Dominion Voting Systems server from a recount center in Fulton County, Georgia.

“Someone went down to the Fulton center where the votes and Dominion machines were, claimed there was a software glitch and they had to replace the software, and it seems that they removed the server,” Powell told “Lou Dobbs Tonight” in an

interview aired on Nov. 30.

Powell added that her team does not know where the server is.

Dominion's software and hardware features prominently in two lawsuits filed by Powell in Georgia and Michigan.

The lawsuits claim that the software is vulnerable to manipulation by hackers and was used to alter to vote totals in the presidential election.

Powell prefaced her comment by saying that the alleged removal of the server took place when her team was seeking a temporary restraining order against the resetting, wiping, or altering of any of the Dominion machines. A district court judge subsequently granted the temporary restraining order on Sunday night.

Powell said her team is making significant progress in both cases while preparing to files suits in other states. She said the lawsuits are meant to stop the runoff elections in Georgia in January "because all the machines are infected with the software code that allows Dominion to shave votes from one candidate and give them to another and other features that do the same thing."

“Different states shaved different amounts of votes. The system was set up to shave and flip different votes in different states. Some people were targeted as individual candidates. It’s really the most massive and historical egregious fraud the world has ever seen,” Powell said.

Dominion has vehemently denied these and other allegations.

A Dominion Voting Systems server crashed on Nov. 29 during the second recount in Georgia, according to a spokesman for Fulton County.

“A newly purchased Dominion mobile server crashed,” the spokesman told The Epoch Times via email. “Technicians from Dominion have been dispatched to resolve the issue.”

The office of the Georgia Secretary of State Brad Raffensperger, a Republican, was told of the issue and is aware of attempts to fix the problem, the spokesman said.

Dominion and Raffensperger’s office didn’t immediately respond to emailed requests for comment.

The judge presiding over the Powell case in Georgia has scheduled a hearing concerning the temporary restraining order for Dec. 4.

According to an affidavit from a GOP poll worker that was filed alongside the request for a restraining order, an election official wrote in a message on Nov. 25 that some ballot-counting machines were to be reset on Nov. 30 so they could be used in the machine recount requested by the Trump campaign given the tight margin with former Vice President Joe Biden.

Upon seeing the message, the poll worker said they notified their supervisor because they were concerned about wiping of the machines.

“I am seeing lots of notices from lawyers about possibly impounding the machines,” the poll worker wrote, according to the affidavit. “Lawyers are now saying that the machines should be confiscated immediately before this happens to protect forensic data. They are saying those machines need to be impounded ASAP. Yikes. Maybe I’m being overly paranoid but let’s be sure this is what we’re supposed to be doing.”

The supervisor responded: “It’s what we are supposed to do. It will take a court

order to stop this process—so I guess we need to keep watching the news. If we get a court order to stop, we will see it in our SOS information.”

When the poll worker asked if the reset will wipe the forensic info from the machines, the manager said that “Atlanta already did it.”

↑ 0 ↓ ○○○

ppaulie

Dec 1st, 2020, 4:47 PM • 143 months •

🗨️ 12,263

GABUSC said... (original post)
would think the Republicans would welcome wiping them clean.The party had whined since the Election took place.Do you really want the same machines ...

[show more](#)

Is this the same as the Russia collusion charge brought to all of us by your side?, just curious.

↑ 0 ↓ ○○○

GABUSC

Dec 1st, 2020, 5:13 PM • 231 months •

🗨️ 8,328

ppaulie said... (original post)*Is this the same as the Russia collusion charge brought to all of us by your side?, just curious.*

[show more](#)

Good to see you acknowledge the machines weren't the fault of any Fraud or Improper False Election Charges.

I wasn't aware Cult Member's had rehab facilities could you fill us in or, you're not allowed to discuss it on a Forum?

GO SC

GO SC



0



ooo

ppaulie

Dec 1st, 2020, 5:36 PM • 143 months •

12,263

GABUSC said... (original post)*Good to see you acknowledge the machines weren't the fault of any Fraud or Improper False Election Charges.I wasn't aware Cult Member's had reha...*

[show more](#)

GABUSC, don't be like Gunnm and spin

and try and change directions, I asked you a question yes or no do you agree or disagree?, don't make a mountain out of a mole hill.

I have far more respect for you than a number of people on this board, have I been wrong?.



0



ooo

Reply

Back To Topics



[ABOUT](#) [CONTACT US](#) [ADVERTISERS](#) [MEMBER SERVICES](#) [CAREERS](#) [CUSTOMER SERVICE](#)

[PRIVACY POLICY](#) [TERMS OF SERVICE](#) [TERMS OF USE](#) [TOGGLE FULL/MOBILE](#)

[CA PRIVACY/INFO WE COLLECT](#) [CA DO NOT SELL MY INFO](#)

sp@rtradar

© 2005-2021 CBS INTERACTIVE ALL RIGHTS RESERVED. CBS Sports is a registered trademark of CBS Broadcasting Inc.

Exhibit 8.

Public Law 86-449

May 6, 1960
[H. R. 8601]

AN ACT

To enforce constitutional rights, and for other purposes.

Civil Rights Act
of 1960.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Civil Rights Act of 1960".

TITLE I

OBSTRUCTION OF COURT ORDERS

62 Stat. 769.

SEC. 101. Chapter 73 of title 18, United States Code, is amended by adding at the end thereof a new section as follows:

"§ 1509. Obstruction of court orders

"Whoever, by threats or force, willfully prevents, obstructs, impedes, or interferes with, or willfully attempts to prevent, obstruct, impede, or interfere with, the due exercise of rights or the performance of duties under any order, judgment, or decree of a court of the United States, shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

"No injunctive or other civil relief against the conduct made criminal by this section shall be denied on the ground that such conduct is a crime."

SEC. 102. The analysis of chapter 73 of such title is amended by adding at the end thereof the following:

"1509. Obstruction of court orders."

TITLE II

FLIGHT TO AVOID PROSECUTION FOR DAMAGING OR DESTROYING ANY BUILDING OR OTHER REAL OR PERSONAL PROPERTY; AND, ILLEGAL TRANSPORTATION, USE OR POSSESSION OF EXPLOSIVES; AND, THREATS OR FALSE INFORMATION CONCERNING ATTEMPTS TO DAMAGE OR DESTROY REAL OR PERSONAL PROPERTY BY FIRE OR EXPLOSIVES

62 Stat. 755.

SEC. 201. Chapter 49 of title 18, United States Code, is amended by adding at the end thereof a new section as follows:

"§ 1074. Flight to avoid prosecution for damaging or destroying any building or other real or personal property

"(a) Whoever moves or travels in interstate or foreign commerce with intent either (1) to avoid prosecution, or custody, or confinement after conviction, under the laws of the place from which he flees, for willfully attempting to or damaging or destroying by fire or explosive any building, structure, facility, vehicle, dwelling house, synagogue, church, religious center or educational institution, public or private, or (2) to avoid giving testimony in any criminal proceeding relating to any such offense shall be fined not more than \$5,000 or imprisoned not more than five years, or both.

"(b) Violations of this section may be prosecuted in the Federal judicial district in which the original crime was alleged to have been committed or in which the person was held in custody or confinement: *Provided, however,* That this section shall not be construed as indicating an intent on the part of Congress to prevent any State, Territory, Commonwealth, or possession of the United States of any jurisdiction over any offense over which they would have jurisdiction in the absence of such section."

SEC. 202. The analysis of chapter 49 of such title is amended by adding thereto the following:

"1074. Flight to avoid prosecution for damaging or destroying any building or other real or personal property."

SEC. 203. Chapter 39 of title 18 of the United States Code is amended by adding at the end thereof the following new section:

62 Stat. 738.

"§ 837. Explosives; illegal use or possession; and, threats or false information concerning attempts to damage or destroy real or personal property by fire or explosives

"(a) As used in this section—

Definitions.

"'commerce' means commerce between any State, Territory, Commonwealth, District, or possession of the United States, and any place outside thereof; or between points within the same State, Territory, or possession, or the District of Columbia, but through any place outside thereof; or within any Territory, or possession of the United States, or the District of Columbia;

"'explosive' means gunpowders, powders used for blasting, all forms of high explosives, blasting materials, fuzes (other than electric circuit breakers), detonators, and other detonating agents, smokeless powders, and any chemical compounds or mechanical mixture that contains any oxidizing and combustible units, or other ingredients, in such proportions, quantities, or packing that ignition by fire, by friction, by concussion, by percussion, or by detonation of the compound or mixture or any part thereof may cause an explosion.

"(b) Whoever transports or aids and abets another in transporting in interstate or foreign commerce any explosive, with the knowledge or intent that it will be used to damage or destroy any building or other real or personal property for the purpose of interfering with its use for educational, religious, charitable, residential, business, or civic objectives or of intimidating any person pursuing such objectives, shall be subject to imprisonment for not more than one year, or a fine of not more than \$1,000, or both; and if personal injury results shall be subject to imprisonment for not more than ten years or a fine of not more than \$10,000, or both; and if death results shall be subject to imprisonment for any term of years or for life, but the court may impose the death penalty if the jury so recommends.

Penalties.

"(c) The possession of an explosive in such a manner as to evince an intent to use, or the use of, such explosive, to damage or destroy any building or other real or personal property used for educational, religious, charitable, residential, business, or civic objectives or to intimidate any person pursuing such objectives, creates rebuttable presumptions that the explosive was transported in interstate or foreign commerce or caused to be transported in interstate or foreign commerce by the person so possessing or using it, or by a person aiding or abetting the person so possessing or using it: *Provided, however,* That no person may be convicted under this section unless there is evidence independent of the presumptions that this section has been violated.

"(d) Whoever, through the use of the mail, telephone, telegraph, or other instrument of commerce, willfully imparts or conveys, or causes to be imparted or conveyed, any threat, or false information knowing the same to be false, concerning an attempt or alleged attempt being made, or to be made, to damage or destroy any building or other real or personal property for the purpose of interfering with its use for educational, religious, charitable, residential, business, or civic objectives, or of intimidating any person pursuing such objectives, shall be subject to imprisonment for not more than one year or a fine of not more than \$1,000, or both.

"(e) This section shall not be construed as indicating an intent on the part of Congress to occupy the field in which this section operates to the exclusion of a law of any State, Territory, Commonwealth, or possession of the United States, and no law of any State, Territory, Commonwealth, or possession of the United States which would be valid in the absence of the section shall be declared invalid, and no local authorities shall be deprived of any jurisdiction over any offense over which they would have jurisdiction in the absence of this section."

SEC. 204. The analysis of chapter 39 of title 18 is amended by adding thereto the following:

"837. Explosives; illegal use or possession; and threats or false information concerning attempts to damage or destroy real or personal property by fire or explosives."

TITLE III

FEDERAL ELECTION RECORDS

SEC. 301. Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election, except that, when required by law, such records and papers may be delivered to another officer of election and except that, if a State or the Commonwealth of Puerto Rico designates a custodian to retain and preserve these records and papers at a specified place, then such records and papers may be deposited with such custodian, and the duty to retain and preserve any record or paper so deposited shall devolve upon such custodian. Any officer of election or custodian who willfully fails to comply with this section shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

SEC. 302. Any person, whether or not an officer of election or custodian, who willfully steals, destroys, conceals, mutilates, or alters any record or paper required by section 301 to be retained and preserved shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

SEC. 303. Any record or paper required by section 301 to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative. This demand shall contain a statement of the basis and the purpose therefor.

SEC. 304. Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this title, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

SEC. 305. The United States district court for the district in which a demand is made pursuant to section 303, or in which a record or paper so demanded is located, shall have jurisdiction by appropriate process to compel the production of such record or paper.

SEC. 306. As used in this title, the term "officer of election" means any person who, under color of any Federal, State, Commonwealth,

"Officer of election."

or local law, statute, ordinance, regulation, authority, custom, or usage, performs or is authorized to perform any function, duty, or task in connection with any application, registration, payment of poll tax, or other act requisite to voting in any general, special, or primary election at which votes are cast for candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico.

TITLE IV

EXTENSION OF POWERS OF THE CIVIL RIGHTS COMMISSION

SEC. 401. Section 105 of the Civil Rights Act of 1957 (42 U.S.C. Supp. V 1975d) (71 Stat. 635) is amended by adding the following new subsection at the end thereof:

“(h) Without limiting the generality of the foregoing, each member of the Commission shall have the power and authority to administer oaths or take statements of witnesses under affirmation.”

TITLE V

EDUCATION OF CHILDREN OF MEMBERS OF ARMED FORCES

SEC. 501. (a) Subsection (a) of section 6 of the Act of September 30, 1950 (Public Law 874, Eighty-first Congress), as amended, relating to arrangements for the provision of free public education for children residing on Federal property where local educational agencies are unable to provide such education, is amended by inserting after the first sentence the following new sentence: “Such arrangements to provide free public education may also be made for children of members of the Armed Forces on active duty, if the schools in which free public education is usually provided for such children are made unavailable to them as a result of official action by State or local governmental authority and it is the judgment of the Commissioner, after he has consulted with the appropriate State educational agency, that no local educational agency is able to provide suitable free public education for such children.”

64 Stat. 1107.
20 USC 241.

(b) (1) The first sentence of subsection (d) of such section 6 is amended by adding before the period at the end thereof: “or, in the case of children to whom the second sentence of subsection (a) applies, with the head of any Federal department or agency having jurisdiction over the parents of some or all of such children”.

(2) The second sentence of such subsection (d) is amended by striking out “Arrangements” and inserting in lieu thereof “Except where the Commissioner makes arrangements pursuant to the second sentence of subsection (a), arrangements”.

SEC. 502. Section 10 of the Act of September 23, 1950 (Public Law 815, Eighty-first Congress), as amended, relating to arrangements for facilities for the provision of free public education for children residing on Federal property where local educational agencies are unable to provide such education, is amended by inserting after the first sentence the following new sentence: “Such arrangements may also be made to provide, on a temporary basis, minimum school facilities for children of members of the Armed Forces on active duty, if the schools in which free public education is usually provided for

72 Stat. 553.
20 USC 640.

such children are made unavailable to them as a result of official action by State or local governmental authority and it is the judgment of the Commissioner, after he has consulted with the appropriate State educational agency, that no local educational agency is able to provide suitable free public education for such children."

TITLE VI

SEC. 601. That section 2004 of the Revised Statutes (42 U.S.C. 1971), as amended by section 131 of the Civil Rights Act of 1957 (71 Stat. 637), is amended as follows:

(a) Add the following as subsection (e) and designate the present subsection (e) as subsection "(f)":

Voting rights.
Court action.

"In any proceeding instituted pursuant to subsection (c) in the event the court finds that any person has been deprived on account of race or color of any right or privilege secured by subsection (a), the court shall upon request of the Attorney General and after each party has been given notice and the opportunity to be heard make a finding whether such deprivation was or is pursuant to a pattern or practice. If the court finds such pattern or practice, any person of such race or color resident within the affected area shall, for one year and thereafter until the court subsequently finds that such pattern or practice has ceased, be entitled, upon his application therefor, to an order declaring him qualified to vote, upon proof that at any election or elections (1) he is qualified under State law to vote, and (2) he has since such finding by the court been (a) deprived of or denied under color of law the opportunity to register to vote or otherwise to qualify to vote, or (b) found not qualified to vote by any person acting under color of law. Such order shall be effective as to any election held within the longest period for which such applicant could have been registered or otherwise qualified under State law at which the applicant's qualifications would under State law entitle him to vote.

"Notwithstanding any inconsistent provision of State law or the action of any State officer or court, an applicant so declared qualified to vote shall be permitted to vote in any such election. The Attorney General shall cause to be transmitted certified copies of such order to the appropriate election officers. The refusal by any such officer with notice of such order to permit any person so declared qualified to vote to vote at an appropriate election shall constitute contempt of court.

"An application for an order pursuant to this subsection shall be heard within ten days, and the execution of any order disposing of such application shall not be stayed if the effect of such stay would be to delay the effectiveness of the order beyond the date of any election at which the applicant would otherwise be enabled to vote.

Voting referees.

23 Stat. 22.

"The court may appoint one or more persons who are qualified voters in the judicial district, to be known as voting referees, who shall subscribe to the oath of office required by Revised Statutes, section 1757; (5 U.S.C. 16) to serve for such period as the court shall determine, to receive such applications and to take evidence and report to the court findings as to whether or not at any election or elections (1) any such applicant is qualified under State law to vote, and (2) he has since the finding by the court heretofore specified been (a) deprived of or denied under color of law the opportunity to register to vote or otherwise to qualify to vote, or (b) found not qualified to vote by any person acting under color of law. In a proceeding before a voting referee, the applicant shall be heard ex parte at such times and places as the court shall direct. His statement under oath shall be prima facie evidence as to his age, residence, and his prior efforts

to register or otherwise qualify to vote. Where proof of literacy or an understanding of other subjects is required by valid provisions of State law, the answer of the applicant, if written, shall be included in such report to the court; if oral, it shall be taken down stenographically and a transcription included in such report to the court.

"Upon receipt of such report, the court shall cause the Attorney General to transmit a copy thereof to the State attorney general and to each party to such proceeding together with an order to show cause within ten days, or such shorter time as the court may fix, why an order of the court should not be entered in accordance with such report. Upon the expiration of such period, such order shall be entered unless prior to that time there has been filed with the court and served upon all parties a statement of exceptions to such report. Exceptions as to matters of fact shall be considered only if supported by a duly verified copy of a public record or by affidavit of persons having personal knowledge of such facts or by statements or matters contained in such report; those relating to matters of law shall be supported by an appropriate memorandum of law. The issues of fact and law raised by such exceptions shall be determined by the court or, if the due and speedy administration of justice requires, they may be referred to the voting referee to determine in accordance with procedures prescribed by the court. A hearing as to an issue of fact shall be held only in the event that the proof in support of the exception disclose the existence of a genuine issue of material fact. The applicant's literacy and understanding of other subjects shall be determined solely on the basis of answers included in the report of the voting referee.

Transmittal of
report and order.

"The court, or at its direction the voting referee, shall issue to each applicant so declared qualified a certificate identifying the holder thereof as a person so qualified.

"Any voting referee appointed by the court pursuant to this subsection shall to the extent not inconsistent herewith have all the powers conferred upon a master by rule 53(c) of the Federal Rules of Civil Procedure. The compensation to be allowed to any persons appointed by the court pursuant to this subsection shall be fixed by the court and shall be payable by the United States.

28 USC app.

"Applications pursuant to this subsection shall be determined expeditiously. In the case of any application filed twenty or more days prior to an election which is undetermined by the time of such election, the court shall issue an order authorizing the applicant to vote provisionally: *Provided, however,* That such applicant shall be qualified to vote under State law. In the case of an application filed within twenty days prior to an election, the court, in its discretion, may make such an order. In either case the order shall make appropriate provision for the impounding of the applicant's ballot pending determination of the application. The court may take any other action, and may authorize such referee or such other person as it may designate to take any other action, appropriate or necessary to carry out the provisions of this subsection and to enforce its decrees. This subsection shall in no way be construed as a limitation upon the existing powers of the court.

"When used in the subsection, the word 'vote' includes all action necessary to make a vote effective including, but not limited to, registration or other action required by State law prerequisite to voting, casting a ballot, and having such ballot counted and included in the appropriate totals of votes cast with respect to candidates for public office and propositions for which votes are received in an election; the words 'affected area' shall mean any subdivision of the State in which the laws of the State relating to voting are or have been to

Definitions.

any extent administered by a person found in the proceeding to have violated subsection (a); and the words 'qualified under State law' shall mean qualified according to the laws, customs, or usages of the State, and shall not, in any event, imply qualifications more stringent than those used by the persons found in the proceeding to have violated subsection (a) in qualifying persons other than those of the race or color against which the pattern or practice of discrimination was found to exist."

State as party
defendant.

(b) Add the following sentence at the end of subsection (c):

"Whenever, in a proceeding instituted under this subsection any official of a State or subdivision thereof is alleged to have committed any act or practice constituting a deprivation of any right or privilege secured by subsection (a), the act or practice shall also be deemed that of the State and the State may be joined as a party defendant and, if, prior to the institution of such proceeding, such official has resigned or has been relieved of his office and no successor has assumed such office, the proceeding may be instituted against the State."

TITLE VII

SEPARABILITY

SEC. 701. If any provision of this Act is held invalid, the remainder of this Act shall not be affected thereby.

Approved May 6, 1960.

Public Law 86-450

May 6, 1960
[S. 1751]

AN ACT

To place in trust status certain lands on the Wind River Indian Reservation in Wyoming.

Wind River In-
dian Reservation,
Wyo.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That all the right, title, and interest of the United States in and to the following-described tracts of land on the Wind River Indian Reservation in Wyoming shall hereafter be held in trust by the United States for the benefit of the Shoshone and Arapahoe Tribes of said reservation:

Section 28, township 1 north, range 1 east, Wind River meridian:

(1) South half, southwest quarter, southwest quarter, northwest quarter, comprising 5.0 acres more or less.

Section 32, township 5 north, range 4 west, Wind River meridian:

(2) Beginning at a point 553.8 feet south of the corner of sections 29, 30, 31, and 32; said point being corner numbered 1; thence south 106.2 feet to corner numbered 2 which is identical with the southwest corner of northwest quarter northwest quarter northwest quarter, section 32; thence east 200 feet to corner numbered 3, thence north 106.2 feet to corner numbered 4; thence west 200 feet to corner numbered 1 and place of beginning, comprising 0.487 acres.

(3) Beginning at a point 118.2 feet south of the corner of sections 29, 30, 31, and 32; said point being corner numbered 1; thence south 435.6 feet to corner numbered 2; thence east 200 feet to corner numbered 3, thence north 435.6 feet to corner numbered 4; thence west 200 feet to point of beginning, or described as a 2-acre tract in the northwest quarter northwest quarter, section 32.

(4) West half southwest quarter northwest quarter northwest quarter, section 32, comprising 5.0 acres.

Approved May 6, 1960.

Exhibit 9.

POLITICO



MAGAZINE

2020

Forget Hanging Chads. Copyright Laws Could be the Next Electoral Quagmire.

Most election-tech equipment is the intellectual property of the companies that make it — meaning a contested election could get even more complicated.



Getty Images

By ISABELLA FARR and OLIVIA REINGOLD
11/03/2020 04:30 AM EST



Isabella Farr is a freelance journalist based in New York, specializing in energy and tech coverage.

Olivia Reingold is an editor-producer for POLITICO Audio.

If you used a mail-in ballot in Fulton County, Georgia this year, you may have noticed peculiar language at the top of the ballot: “Copyright © 2020 Dominion Voting Inc.” Dominion Voting is a private company that sells election technology. And this ballot design — which was created by Dominion and counted using the company’s proprietary equipment — is technically its intellectual property.

Unusual as it may seem, this isn’t uncommon: Most voting technology used throughout the U.S. is covered by intellectual property law. That means the touch-screen you might have tapped on to vote could be patented. The software used to process your vote could be copyrighted. Before you even got to the voting booth, your ballot was likely designed on copyrighted software.

Advertisement

And all of it could cause a nightmare after Nov. 3, according to election-security experts.

“We’re going to wind up with a thousand court cases that cannot just be resolved by just going into the software and checking to see what happened, because it’s proprietary,” said Ben Ptashnik, the co-founder of the [National Election Defense Coalition](#), a bipartisan advocacy group that pushes Congress to reform election security.

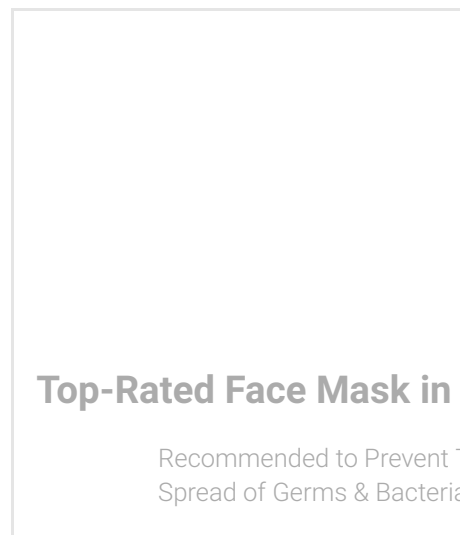
POLITICO DISPATCH:NOVEMBER 3

Election Day is here. The results? They might not be finalized for a while. And that has lawyers for Trump and Biden preparing for lawsuits, recounts and some odd scenarios that you might never have thought of.



Subscribe on Apple Podcasts | Subscribe on Google Podcasts

In most elections, the intellectual-property laws that surround the machinery of America’s electoral system prove inconsequential in determining who won or lost a campaign, and software isn’t central to most contested-election scenarios, such as late-arriving ballots or issues with access to polling locations. But in instances where the vote tally itself is in question, analysts could need access to voting machines’ underlying code to determine if potential security flaws, errors or even purposeful tampering are behind the irregularities. And this year, with widespread fears of contested ballots, recounts and the potential for weeks of legal challenges that threaten to undermine public faith in the results, those IP laws could prove decisive.



Advertisement

“You know how Apple fights against law enforcement coming in and going into their iPhone software? Well, you’d be in the same position,” said Ptashnik. “You might have to go all the way to the Supreme Court to get permission to get into proprietary software.”

Three major companies — Election Systems & Software, Dominion Voting Systems and Hart InterCivic — together control about 90 percent of the U.S. market for voting systems, according to election security advocates and researchers consulted by POLITICO. Industry-wide, it is standard practice for those companies to tightly control who has access to their proprietary software — not only to help those companies maintain an edge over their competitors, but to prevent the fraud or hacking of elections equipment. That means that the relevant source code used to design ballots and tabulate votes is copyrighted and private.

The rough outline of those legal battles is further complicated by the contracts some states have entered into with the election-tech companies. For instance, take Michigan — the pivotal battleground state that President Donald Trump won in 2016. Under a [10-year contract signed with Hart InterCivic](#) in 2017, the

state agreed not to “attempt to access or derive any source code” used by the company. In a [similar agreement with Dominion](#), Michigan “agree[d] not to reverse engineer or otherwise attempt to derive the source code” of the company’s software, and forfeited its right to transfer its license for Dominion’s software to third parties.

Contracts and licensing agreements are one of a few ways companies prevent outsiders from looking at their proprietary code. The Digital Millennium Copyright Act is another. Section 1201 of that federal law may block anyone besides the source code owner from accessing and viewing copyrighted source code, even if it’s for the purpose of gauging the security of those systems.

For researchers like University of Michigan computer science professor J. Alex Halderman, that presents a real obstacle.

“I’ve studied machines several times that came up on eBay after state governments decommissioned them,” said Halderman. “Once, in 2005, I got to study another voting machine because an anonymous source gave us one and our lawyers were convinced we would be allowed to study it.”

AD

What Halderman and others are trying to prove is that these machines are

secure. But some election technology companies say giving researchers access to their software is a security risk in itself.

Voatz, a technology firm that sells mobile voting systems, recently filed an [amicus brief to the Supreme Court](#) arguing that opening up its software to well-meaning third parties invites bad actors to exploit the system.

“If a security vulnerability is widely disseminated publicly and prematurely, it can expose software platforms and their users to malicious attacks, as ill-intentioned hackers can take advantage of such vulnerabilities prior to the development of any patch,” the brief said.

There are other ways to ensure security besides opening the door to hackers. One option is certifying technology equipment through the Election Assistance Commission, which also tests systems for functionality and accessibility. But Halderman says its testing program is weak.

“That level of testing is very superficial from a security standpoint,” Halderman said. “There’s now been many, many dozens of studies by academics and other independent researchers of voting machines in the U.S., virtually every one of which passed the EAC testing before it was found to have vulnerabilities by other testers.”

Federal auditors do get to inspect parts of voting-machine software, but the goal is to evaluate functionality, not quality, according to Eddie Perez, a former Hart InterCivic executive who now works with the [Open Source Election Technology Institute](#) to advocate for publicly owned voting systems.

“It’s a little bit like a mechanic looking under the hood of a car and saying, ‘The carburetor is indeed driving the piston, and that’s driving the crankshaft that makes the wheels go,’” said Perez. “But that’s not the same thing as the mechanic saying, ‘This is the best-quality car that I’ve ever seen and it’s a

Mercedes, not a Yugo.”

Getting that sort of third-party certification is critical to building public trust in an election’s outcome, said Perez. Without it, the public might have a hard time trusting election officials or election-technology companies — both of which could hypothetically produce an audit that protects their own interests.

AD

Dominion and Hart InterCivic did not respond to repeated requests for comment for this article. ES&S told POLITICO its systems have been inspected by third parties, but it's unclear if those audits were paid for by the company and if the findings were made public.

“ES&S has been participating in an industry effort to craft a vulnerability disclosure program that works for both security researchers and the elections technology industry,” a company spokesperson said. That [program invites findings from researchers](#) about possible vulnerability in its digital products, even though ES&S “does not give authorization to test state and local government election related networks or assets.”

Asked why it frequently places its products under intellectual protection, ES&S had a simple answer: “It’s common practice for businesses to protect their intellectual property.”

Which, to election security experts, is precisely the problem.

“What is so secret about the way these machines are counting our votes?” asked Halderman. “That’s the question that everyone should be asking when we’re told that the software is copyrighted.”

Exhibit 10.



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

An Introduction to Hiding and Finding Data on Linux

GIAC Security Essentials Certification (GSEC)

Practical Assignment Version 1.4b - Option 1

Gary Robertson

Table of Contents

| | |
|--|-----------|
| ABSTRACT | 2 |
| INTRODUCTION | 2 |
| FORENSIC SOFTWARE INSTALLATION | 2 |
| INSTALLATION OF THE SLEUTH KIT | 2 |
| INSTALLATION OF AUTOPSY | 3 |
| HIDDEN DIRECTORIES | 3 |
| HIDING DATA IN HIDDEN DIRECTORIES | 3 |
| FINDING DATA IN HIDDEN DIRECTORIES | 4 |
| <i>Using Linux Utilities</i> | 4 |
| CAMOUFLAGED FILES | 5 |
| HIDING DATA WITH CAMOUFLAGE | 5 |
| FINDING DATA HIDDEN WITH CAMOUFLAGE | 6 |
| <i>Using Linux Utilities</i> | 6 |
| <i>Using The Sleuth Kit / Autopsy</i> | 6 |
| DELETING FILES | 7 |
| HIDING DATA BY DELETING FILES | 8 |
| FINDING DATA IN DELETED FILES | 8 |
| <i>Using Linux Utilities</i> | 8 |
| <i>Using The Sleuth Kit / Autopsy</i> | 9 |
| UNLINKING OPEN FILES | 11 |
| HIDING DATA VIA UNLINKING AN OPEN FILE | 11 |
| FINDING DATA HIDDEN VIA UNLINKING AN OPEN FILE | 13 |
| <i>Using The Sleuth Kit / Autopsy</i> | 13 |
| SLACK SPACE | 14 |
| HIDING DATA IN SLACK SPACE | 14 |
| FINDING DATA HIDDEN IN SLACK SPACE | 16 |
| <i>Using Linux Utilities</i> | 16 |
| <i>Using The Sleuth Kit / Autopsy</i> | 16 |
| APPENDIX | 19 |
| CREATING A FORENSIC IMAGE | 19 |
| REFERENCES | 20 |

Abstract

This paper provides an introduction to several of the common techniques for hiding data on Linux systems (specifically those using the ext2 file system), as well as some methods for finding hidden data on these systems. The techniques of hiding directories, camouflaging files, deleting files, unlinking open files and using file slack space are explained with a focus on simple, step-by-step examples. For each of these data hiding techniques there is a corresponding section that provides an example-led approach to finding the data. Aside from using Linux commands to find hidden data, some basic computer forensics techniques are presented using the open source tools of The Sleuth Kit and its companion browser-based interface, Autopsy.

Introduction

The techniques outlined in this paper are aimed at educating beginners in the fields of system administration or computer forensics as to how data may be hidden on systems, and how one may go about finding this data. The paper is not meant to be a guide for real-world investigations. In particular, the data finding sections do not represent best practice in the area of computer forensics. For the sake of simplicity the forensic images are copied onto the same system that houses the "evidence", thereby breaking one of the basic rules of computer forensics (Shinder, p.552). Nevertheless, the example-led approach to explaining the techniques should provide a valuable starting point for people interested in data hiding on Linux systems.

This paper does not cover two important methods of data hiding, encryption and steganography. Both of these methods rely on specific algorithms, which often vary from application to application. They are not methods that are peculiar to Linux or other UNIX-like operating systems, and for this reason they have been excluded from the discussion.

All of the examples in this paper have been carried out on a system running Red Hat Linux version 8.0, using the ext2 file system rather than the default ext3 file system. Except where noted, all of the data hiding techniques have been performed by user "sans", whose home directory is /home/sans. All of the techniques for finding hidden data have been performed by the superuser, "root". The Linux examples will often show a command prompt that includes the user name, the machine name (always "tortilla") and the current directory name. For example, a prompt such as "[root@tortilla /]#" indicates the superuser working in the base directory of the system. The final character in the prompt will always be a "#" for the superuser and a "\$" for the user "sans".

Forensic Software Installation

Some of the demonstrations for finding hidden data require the use of forensic software tools. For this reason a quick discussion of these tools is provided before starting on the demonstrations.

Installation of The Sleuth Kit

The Sleuth Kit is an open source forensic toolkit that has its origins in a group of file system analysis tools by Wietse Venema and Dan Farmer called The Coroner's Toolkit

(TCT). Up until quite recently the toolkit went under the name of TASK, an acronym for The @stake Sleuth Kit. The person now in charge of development is Brian Carrier, with the current version being 1.61. The Web site for The Sleuth Kit is:

<http://www.sleuthkit.org/sleuthkit/index.php>

To install The Sleuth Kit, download the compressed file from the Web site, unpack it in a directory on your Linux machine (I have created a directory of /usr/local/security for this purpose), and follow the directions in the INSTALL file. Make sure to create a soft link to the directory created during the unpacking by entering a command such as:

```
ln -s sleuthkit-1.61 sleuthkit
```

Installation of Autopsy

Autopsy is a companion program to the Sleuth Kit. Autopsy makes it easier to work with the many tools provided with the Sleuth Kit by providing a graphical interface to those tools in the form of a browser. At the time of writing, the current version of Autopsy is 1.71, and its Web site is:

<http://www.sleuthkit.org/autopsy/index.php>

The instructions for installing Autopsy are very similar to those for The Sleuth Kit: download the compressed file from the Web site, unpack it in a directory on your Linux machine, and follow the directions in the INSTALL file. As for The Sleuth Kit, I unpacked Autopsy into my /usr/local/security directory and created a soft link to the resultant directory using the `ln` command:

```
ln -s autopsy-1.71 autopsy
```

The Autopsy installation prompts for an "Evidence Locker Directory". This is the base directory for storage of files for forensic investigation. I created a directory of /usr/local/forensics for this purpose.

Hidden Directories

This is a basic method of hiding data that relies on the non-discovery of the directory containing the data. The actual data files are often not disguised in any way; the effort instead going into hiding the directory itself. There are two main approaches to accomplishing this. The first approach involves giving the directory a strange name that may go unnoticed on file listings, whilst the second approach involves creating the directory in a part of the system where it is least likely to be found by a system administrator.

Hiding Data in Hidden Directories

There are a couple of strange directory names that are used over and over by hackers and others who want to conceal data. They are "... " (three dots) and ".. " (two dots and a space). I used these classic directory names to hide data in subdirectories under my /home/sans/dir directory. The commands used to create the directories were:

```
[sans@tortilla dir]$ mkdir ...
[sans@tortilla dir]$ mkdir ".. "
```

I also created a normal directory called "accounts" and placed some Perl script files in all three directories. A simple listing of my /home/sans/dir directory fails to show the hidden directories as they both begin with a dot:

```
[sans@tortilla dir]$ ls -l
total 5
drwxrwxr-x    2  sans      sans      1024 May 21 12:28 accounts
-rw-rw-r--    1  sans      sans         15 May 21 12:27 file1.txt
-rw-rw-r--    1  sans      sans      1568 May 21 12:27 file2.txt
-rw-rw-r--    1  sans      sans       167 May 21 12:27 file3.txt
```

A full listing of the same directory reveals the hidden directories, but they may go unnoticed due to their similarity in the listing with the current and parent directories (represented by a single dot and two dots respectively):

```
[sans@tortilla dir]$ ls -al
total 9
drwxrwxr-x    5  sans      sans      1024 May 21 12:27 .
drwx-----    4  sans      users      1024 May 21 12:27 ..
drwxrwxr-x    2  sans      sans      1024 May 21 12:29 ..
drwxrwxr-x    2  sans      sans      1024 May 21 12:28 ...
drwxrwxr-x    2  sans      sans      1024 May 21 12:28 accounts
-rw-rw-r--    1  sans      sans         15 May 21 12:27 file1.txt
-rw-rw-r--    1  sans      sans      1568 May 21 12:27 file2.txt
-rw-rw-r--    1  sans      sans       167 May 21 12:27 file3.txt
```

The other approach to hiding directories, that of creating the directory in a seldomly traversed part of the system, is fairly simple to comprehend, so I will not demonstrate it here. Note, however, that the /dev directory is one of the most frequently used locations to hide other directories (Green, p. 35). This is because the hidden directory can go unnoticed amongst the hundreds of other files and directories in this location.

Finding Data in Hidden Directories

Using Linux Utilities

The find command with various options can be used to clearly show directories which have been hidden by giving them a prefix of ".":

```
[root@tortilla dir]# find /home/sans -type d -name ".*" -print
/home/sans/.kde
/home/sans/dir/...
/home/sans/dir/..
```

The "-type d" option in the above command limits output to directories only. In addition to the two directories that were created earlier, the output shows a directory named ".kde". This directory has been created by the KDE application, and can be ignored for the purposes of this demonstration.

The following command (split over two lines for presentation purposes) not only outputs the directories, but also the data files that reside in these directories. Note that in this command the "-print0" and "-0" are important - without them the shell interprets the directory of ".. " (two dots and a space) as the parent directory "." (two dots):

```
[root@tortilla dir]# find /home/sans -type d -name ".*" \
-print0 | xargs -0 ls -l
/home/sans/dir/.. :
total 5
-rw-r--r--    1 sans      sans      1070 May 21 12:29 common.pl
-rw-r--r--    1 sans      sans        554 May 21 12:29 edit.pl
-rw-r--r--    1 sans      sans      1039 May 21 12:29 show.pl

/home/sans/dir/...:
total 3
-rw-r--r--    1 sans      sans       342 May 21 12:28 index.pl
-rw-r--r--    1 sans      sans      1147 May 21 12:28 search.pl

/home/sans/.kde:
total 1
drwxr-xr-x    2 sans      users     1024 Jun 30  2003 Autostart
```

A system administrator wishing to periodically check for hidden directories could create a cron job containing a similar `find` command. However, the command would fail to find directories with names that do not begin with a dot, but have instead been hidden in a seldomly traversed part of the system. Therefore perhaps the best method for system administrators to counter the subterfuge of hidden directories is by using a file integrity checker such as Tripwire to report on directory creation.

Camouflaged Files

This is a basic method of hiding data that relies only on the file name. Files containing forbidden data are simply given names implying legitimacy. In particular, the file extension is changed. For example, an employee trying to hide downloaded MP3 audio files or pornography image files under their account may fool a novice system administrator by giving the files innocuous names and changing the file extensions to ".doc".

Hiding Data with Camouflage

As mentioned above, this technique simply requires changing filenames. I found several image, audio and document files and placed them in my `/home/sans/cam` directory as shown:

```
[sans@tortilla cam]$ ls -l
total 422
-rw-rw-r--    1 sans      sans     136617 May 21 13:14 beach.jpg
-rw-rw-r--    1 sans      sans     21077 May 21 13:14 book.gif
-rw-rw-r--    1 sans      sans     83260 May 21 13:14 forest.jpg
-rw-rw-r--    1 sans      sans     95668 May 21 13:14 gong.wav
-rw-rw-r--    1 sans      sans     37376 May 21 13:14 report1.doc
-rw-rw-r--    1 sans      sans     19335 May 21 13:14 table.gif
-rw-rw-r--    1 sans      sans     28380 May 21 13:14 train.wav
```

I then changed the filenames of three of the files (`beach.jpg`, `table.gif` and `train.wav`) to

camouflage the data that they contained. All of these camouflaged files were given the prefix of "cam" for demonstration purposes. These image and audio files now appear at first glance to contain word processing documents:

```
[sans@tortilla cam]$ ls -l
total 422
-rw-rw-r-- 1 sans      sans      21077 May 21 13:14 book.gif
-rw-rw-r-- 1 sans      sans      19335 May 21 13:14 cam_report1.doc
-rw-rw-r-- 1 sans      sans    136617 May 21 13:14 cam_report2.doc
-rw-rw-r-- 1 sans      sans    28380 May 21 13:14 cam_report3.doc
-rw-rw-r-- 1 sans      sans    83260 May 21 13:14 forest.jpg
-rw-rw-r-- 1 sans      sans    95668 May 21 13:14 gong.wav
-rw-rw-r-- 1 sans      sans    37376 May 21 13:14 report1.doc
```

Finding Data Hidden with Camouflage

Using Linux Utilities

Linux provides a command called `file` that can be used to determine the file type. The man page for this command states that it "uses a combination of file system tests, magic number tests, and language tests" to classify the file. The tests are carried out in that order, with the command terminating on the first successful test. The magic number tests rely on particular file formats containing a consistent binary identifier at the same offset within the file. The output from running the `file` command in my directory containing camouflaged files is:

```
[root@tortilla cam]# file *
book.gif:      GIF image data, version 87a, 640 x 480,
cam_report1.doc: GIF image data, version 87a, 640 x 480,
cam_report2.doc: JPEG image data, JFIF standard 1.02, resolution (DPI), 72 x 72
cam_report3.doc: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit,
mono 11025 Hz
forest.jpg:    JPEG image data, JFIF standard 1.01, resolution (DPI), 72 x 72
gong.wav:      RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit,
mono 11025 Hz
report1.doc:    Microsoft Office Document
```

The `file` command has identified the three camouflaged files as containing image or audio data rather than document data. It should be noted, however, that the command is not foolproof. For example, it is possible to use a hex editor to alter specific bytes within a file, causing the `file` command to classify it incorrectly. This somewhat advanced technique is outside the scope of this paper.

Using The Sleuth Kit / Autopsy

The Sleuth Kit includes a tool called `sorter` that can be used to find camouflaged files. Although it can be run from the command line, it is easier to run via Autopsy. The brief instructions for accomplishing this are:

- 1 Create an image of the partition as set out in the appendix "Creating a Forensic Image".
- 2 Run Autopsy in a browser and create a case and a host name for investigation of the image – my case is called "sans" and its originating host is "tortilla". A symbolic link should be created in a subdirectory of the Autopsy Evidence Locker Directory to link to the forensic image (a HTML form is provided for this). In my example it resulted in

a link from /usr/local/forensics/sans/tortilla/images/dev_hda7.img to the image contained at /usr/local/forensics/dev_hda7.img.

- 3 From the main Autopsy menu, choose "File Type", then choose the link "Sort Files by Type". Ensure that the only checked box is "Extension and File Type Validation", then choose "OK". The `sorter` command will then be run, with Autopsy providing the full path to an index.html file which will help in analysing the results.
- 4 Paste the index.html file into another browser window and click on the link to "Extension Mismatches". My browser's output included two of the three camouflaged files:

```
/mnt/forensics/home/sans/cam/cam_report1.doc
GIF image data, version 87a, 640 x 480 (Ext: doc)
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img Inode: 32130
```

```
/mnt/forensics/home/sans/cam/cam_report2.doc
JPEG image data, JFIF standard 1.02, resolution (DPI), 72 x 72 (Ext: doc)
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img Inode: 32131
```

Note that the `sorter` tool has not reported `cam_report3.doc` as having an extension mismatch, despite the fact that it is really an audio file with a `.wav` extension. This is just a configuration issue. By default the `sorter` tool when run under Linux uses the configuration files of `default.sort` and `linux.sort`, neither of which lists the `.wav` extension as a known category. After copying the appropriate rule set from the provided `windows.sort` file to `linux.sort`, the output of `sorter` was able to identify all of the camouflaged files:

```
/mnt/forensics/home/sans/cam/cam_report1.doc
GIF image data, version 87a, 640 x 480 (Ext: doc)
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img Inode: 32130
```

```
/mnt/forensics/home/sans/cam/cam_report3.doc
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 11025 Hz
(Ext: doc)
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img Inode: 32132
```

```
/mnt/forensics/home/sans/cam/cam_report2.doc
JPEG image data, JFIF standard 1.02, resolution (DPI), 72 x 72 (Ext: doc)
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img Inode: 32131
```

The `sorter` tool could also have been run from the command line. The `man` page for `sorter` explains the various arguments required to run it. Of particular note, however, is the optional `"-e"` argument, which restricts the checks to extension mismatches only. I identified my camouflaged files with the following command:

```
[root@tortilla sleuthkit]# ./bin/sorter -h -m '/mnt/forensics/home/' -d \
'/usr/local/forensics/sans/tortilla/output/sorter-dev_hda7.img/' -f \
linux-ext2 -e '/usr/local/forensics/sans/tortilla/images/dev_hda7.img'
```

Deleting Files

Of course one of the most basic methods of hiding data is simply to delete the file containing the data. In the `ext2` file system the data concerned does not immediately disappear from the hard disk. Instead, the file system merely marks the relevant area on the hard disk as being available for use. Depending on several factors such as the amount

of free space on the disk and the level of disk activity, it may take a significant amount of time before that part of the disk is reclaimed by another file, thus destroying the original data. Taking these factors into account, there exists the possibility of recovering the contents of a deleted file and therefore finding the hidden data. Note that file deletion is handled differently under the newer ext3 file system; the block pointers in the file's inode are cleared, making recovery significantly more difficult ("Linux ext3 FAQ"). The recovery techniques outlined below are specifically for the ext2 file system.

Hiding Data by Deleting Files

People wishing to *temporarily* hide large amounts of data on a system would rarely choose the method of file deletion due to the potential difficulties in recovering all of the data intact. However, it is a method often used by people who wish to *permanently* hide data. Oftentimes users of UNIX-like systems in the workplace are told by Computer Support staff that files erroneously deleted cannot be recovered; they can only be retrieved from backups. These users may therefore form the impression that on Linux and UNIX systems where backups are not routinely performed (such as systems at home), they can permanently remove information from their hard disk by simple file deletion. The fact is that computer data are surprisingly resilient, and there is a good chance that at least some of the deleted data can be recovered (Crane).

To demonstrate hiding and finding data by file deletion I created a directory called /home/sans/del. In this directory I placed two files, one of 1250 bytes and one of 20000 bytes. The files were given names to indicate how many blocks (of 1024 bytes) they should take up on the disk:

```
[sans@tortilla del]$ ls -l two_blocks.txt
-rw-r--r-- 1 sans sans 1250 May 21 16:25 two_blocks.txt

[sans@tortilla del]$ ls -l twenty_blocks.txt
-rw-r--r-- 1 sans sans 20000 May 21 16:25 twenty_blocks.txt
```

As the idea was to delete these files and then attempt to recover them, I ran the `md5sum` tool on the files to generate a 128-bit message digest for later comparison. I then deleted the files with the `rm` command:

```
[sans@tortilla del]$ md5sum two_blocks.txt
e03ebe17c915edd1ee7bbcda09b2baeb two_blocks.txt

[sans@tortilla del]$ md5sum twenty_blocks.txt
69405efd08f20c77b6842c0cb6999e8f twenty_blocks.txt

[sans@tortilla del]$ rm two_blocks.txt
[sans@tortilla del]$ rm twenty_blocks.txt
```

Finding Data in Deleted Files

Using Linux Utilities

The Red Hat Linux distribution includes a file system debugging tool for the ext2 file system called `debugfs` that can be used to recover deleted files consisting of twelve or

fewer disk blocks. I decided to use this tool to see if I could recover the deleted file named `two_blocks.txt`. Firstly I unmounted the `/dev/hda7` partition (`/home`) and created a forensic image to work with, as outlined in the appendix "Creating a Forensic Image". Although the `debugfs` tool does not necessarily require an image (it can work on the partition whilst it remains mounted), creating an image as soon as possible after deleting a file will increase the chances of being able to recover the file intact. Upon running `debugfs`, I requested to see a list of the deleted inodes by entering `lsdel` at the prompt:

```
[root@tortilla root]# debugfs /usr/local/forensics/dev_hda7.img
debugfs 1.27 (8-Mar-2002)
debugfs: lsdel
Inode  Owner  Mode    Size    Blocks    Time deleted
36150   520 100644   1250    2/ 2 Wed May 21 17:00:13 2003
36149   520 100644  20000  21/ 21 Wed May 21 17:00:17 2003
36146   520 100644   7500    8/ 8 Wed May 21 18:57:31 2003
36147   520 100644   3750    4/ 4 Wed May 21 18:57:37 2003
36148   520 100644  10000  10/ 10 Wed May 21 18:57:39 2003
16074   520 100600    959    1/ 1 Wed May 21 19:11:53 2003
38156   520 100600  12288  12/ 12 Wed May 21 19:11:53 2003
38155   520 100664    113    1/ 1 Wed May 21 19:25:41 2003
16075   520 100600    53     1/ 1 Wed May 21 19:28:17 2003
9 deleted inodes found.
```

Fortunately I knew from the file sizes that the first inode listed (36150) referred to the file `two_blocks.txt` that I deleted earlier. I then ran the `stat` command to display the contents of this inode:

```
debugfs: stat <36150>
Inode: 36150  Type: regular      Mode: 0644  Flags: 0x0  Generation: 254443
User: 520    Group: 520    Size: 1250
File ACL: 0  Directory ACL: 0
Links: 0    Blockcount: 4
Fragment:  Address: 0    Number: 0    Size: 0
ctime: 0x3ecc3d3d -- Wed May 21 17:00:13 2003
atime: 0x3ecc3a2d -- Wed May 21 16:47:09 2003
mtime: 0x3ecc352c -- Wed May 21 16:25:48 2003
dtime: 0x3ecc3d3d -- Wed May 21 17:00:13 2003
BLOCKS:
(0-1):147745-147746
TOTAL: 2
```

I then ran the `dump` command within `debugfs` to dump the contents of the inode to a file in my `/tmp` directory. This file should be identical to the deleted file `two_blocks.txt`. I then exited from `debugfs` and confirmed the successful file recovery with the `md5sum` command:

```
debugfs: dump <36150> /tmp/two_blocks.rec
debugfs: quit

[root@tortilla root]# ls -l /tmp/two_blocks.rec
-rw-r--r-- 1 root root 1250 May 22 11:42 /tmp/two_blocks.rec

[root@tortilla root]# md5sum /tmp/two_blocks.rec
e03ebe17c915eddlee7bbcd09b2baeb /tmp/two_blocks.rec
```

Using The Sleuth Kit / Autopsy

As the `debugfs` tool is inappropriate to recover files of more than twelve blocks in size, I

used Autopsy to attempt to recover the deleted file twenty_blocks.txt. The brief instructions for accomplishing this are:

- 1 Create an image of the partition as set out in the appendix "Creating a Forensic Image".
- 2 Assuming that a case and a host name have already been set up during the earlier section on camouflaged files, choose "File Analysis" from the main menu and click on the "All Deleted Files" button to show a listing of deleted files with details such as file type, file name, MAC times (modification, access and inode change times), file size, and inode number. The inode number (appearing under the column "Meta") for the file twenty_blocks.txt is 36149.
- 3 Choose "Meta Data" from the Autopsy main menu and enter in the inode number obtained from the previous step. The output is interesting because it shows that the file actually takes up 21 blocks on the disk, one of them being an indirect block. In the ext2 file system, the inode requires the use of indirect blocks to store the block numbers of all but the first twelve blocks of a file (Crane). In my example the block numbered 147736 contains no data for the file, but instead contains the block numbers for the final eight data blocks of the file (147737 - 147744):

```
Pointed to by file:
inode not currently used
File Type:
ASCII C program text
MD5:
69405efd08f20c77b6842c0cb6999e8f
Details:
inode: 36149
Not Allocated
Group: 18
uid / gid: 520 / 520
mode: -rw-r--r--
size: 20000
num of links: 0

Inode Times:
Accessed: Thu May 22 02:47:17 2003
File Modified: Thu May 22 02:25:48 2003
Inode Modified: Thu May 22 03:00:17 2003
Deleted: Thu May 22 03:00:17 2003

Direct Blocks:
147724 147725 147726 147727 147728 147729 147730 147731
147732 147733 147734 147735 147737 147738 147739 147740
147741 147742 147743 147744

Indirect Blocks:
147736
```

- 4 In order to recover the contents of inode 36149, I then clicked on the "Export Contents" button and saved the file to /tmp/twenty_blocks.rec. Finally I confirmed that the recovered file was identical to the original by running the md5sum command and comparing it to the message digest obtained earlier:

```
[root@tortilla root]# ls -l /tmp/twenty_blocks.rec
-rw----- 1 root root 20000 May 22 13:57 /tmp/twenty_blocks.rec

[root@tortilla root]# md5sum /tmp/twenty_blocks.rec
69405efd08f20c77b6842c0cb6999e8f /tmp/twenty_blocks.rec
```

Although I was successful in recovering both of the deleted files, this is in no way guaranteed by the ext2 file system. Some of the factors that lower the chances of file recovery are large file sizes, high levels of disk fragmentation and high use of the system by multiple users (Crane).

Unlinking Open Files

This is a strategy often used by sniffing programs to log information such as passwords to a file whilst minimising the chances of that file being discovered by a system administrator. It involves a process first opening a file for logging purposes, then calling the `unlink` function on this file, and then writing information to the file. The ext2 file system (along with all major UNIX-like file systems) will keep a lock on the resources used by the file descriptor until either the process exits or the file descriptor is closed (Green p.37). This means that although the file name will not appear on any listings done on the system, its data is protected from being overwritten. The person running the process can therefore return at a later time to collect the logged information, content that their efforts have caused minimal changes to the file system.

Hiding Data via Unlinking an Open File

I created a directory of `/home/sans/unlink` with which to experiment with this method. In this directory I placed a small text file that simulates the user and password information that may be collected by a sniffing program:

```
[sans@tortilla unlink]$ cat junk1.txt
user: tim          passwd: tim123
user: dawn         passwd: dawn123
user: david        passwd: david123
user: gareth       passwd: gareth123
```

I also placed into this directory a small C program that demonstrates the unlinking of an open file. This program was copied from Bach (p.137) with only one alteration of note (mentioned within the source code):

```
[sans@tortilla unlink]$ cat testdel.c
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>

main(int argc, char **argv)
{
    int fd;
    char buffer[1024];
    struct stat statbuf;

    if (argc != 2) {
        /* Sorry, I need a filename to delete */
        printf("Error: No filename provided.\n");
        exit();
    }

    fd = open(argv[1], O_RDONLY);

    if (fd == -1) {
```

```

/* Can't open file */
printf("Error: Cannot open file %s\n", argv[1]);
exit();
}

if (unlink(argv[1]) == -1) {
/* Can't unlink the file */
printf("Error: Cannot unlink file %s\n", argv[1]);
exit();
}
else {
printf("File has been unlinked.\n");
}

/* Check the file by its name */
if (stat(argv[1], &statbuf) == -1) {
printf("stat %s fails as it should.\n", argv[1]);
}
else {
printf("stat %s succeeded!\n", argv[1]);
}

/* Check the file by its file descriptor */
if (fstat(fd, &statbuf) == -1) {
printf("fstat %s fails!\n", argv[1]);
}
else {
printf("fstat %s succeeds as it should.\n", argv[1]);
}

/* Added by G Robertson for demo purposes. */
printf("Pause for 300 seconds, then output file...\n\n");
sleep(300);

/* Read open but deleted file */
while (read(fd, buffer, sizeof(buffer)) > 0) {
printf("%1024s", buffer);
}
}
}

```

Although this program does not write data to a file in the manner explained earlier, it is sufficient to demonstrate the concept of unlinking an open file. The program expects the file name of an existing file to be provided as its only argument. The file is opened with the code "fd = open(argv[1], O_RDONLY)", and is later unlinked with the code "unlink(argv[1])". I added a couple of lines of code to the original program so that it pauses for a few minutes during execution. This provides me with some time to try and detect the process (before it completes) using operating system tools. I compiled the program with the following command:

```
[sans@tortilla unlink]$ gcc -o testdel testdel.c
```

A file listing of the directory after compilation shows the source and executable files for the program, along with the test file:

```

[sans@tortilla unlink]$ ls -l
total 17
-rw-rw-r-- 1 sans      sans      113 May 21 19:01 junk1.txt
-rwxrwxr-x 1 sans      sans      1280 May 21 19:03 testdel
-rw-r--r-- 1 sans      sans      1250 May 21 18:59 testdel.c

```

I ran the program with the command that follows, and quickly moved on to the next section to try and detect the file that had been unlinked:

```
[sans@tortilla unlink]$ ./testdel junk1.txt
File has been unlinked.
stat junk1.txt fails as it should.
fstat junk1.txt succeeds as it should.
Pause for 300 seconds, then output file...
```

```
user: dawn          passwd: dawn123
user: david         passwd: david123
user: gareth        passwd: gareth123

                                user: tim          passwd: tim123
```

Finding Data Hidden via Unlinking an Open File

Using The Sleuth Kit / Autopsy

I performed this search during the five minutes that the `testdel` program was paused. The object of the search was the contents of the file `junk1.txt`. This file no longer appeared on the directory listing, as it had been unlinked early on in the program:

```
[root@tortilla sleuthkit]# cd /usr/local/security/sleuthkit

[root@tortilla sleuthkit]# ls -l /home/sans/unlink/
total 16
-rwxrwxr-x    1 sans      sans      12880 May 21 19:03 testdel
-rw-r--r--    1 sans      sans      1250 May 21 18:59 testdel.c
```

I used the Sleuth Kit's `ils` tool to assist me in the search for the hidden data. The `ils` tool by default lists the inodes of removed files, and by using the `"-o"` option the output is limited to the files that are still open or executing. I entered the following command to search on the `/dev/hda7` partition (`/home`), specifying `linux-ext2` as the relevant file system:

```
[root@tortilla sleuthkit]# ./bin/ils -of linux-ext2 /dev/hda7
class|host|device|start_time
ils|tortilla|/dev/hda7|1053580871
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_dtime|st_mode|st_nli
nk|st_size|st_block0|st_block1
1|a|0|0|1056989311|1056989311|1056989311|0|0|0|0|0|0
3|a|0|0|0|0|0|0|0|0|0|0|0|0
4|a|0|0|0|0|0|0|0|0|0|0|0|0
5|a|0|0|0|0|0|0|0|0|0|0|0|0
6|a|0|0|0|0|0|0|0|0|0|0|0|0
7|a|0|0|0|0|0|0|0|0|0|0|0|0
8|a|0|0|0|0|0|0|0|0|0|0|0|0
9|a|0|0|0|0|0|0|0|0|0|0|0|0
10|a|0|0|0|0|0|0|0|0|0|0|0|0
38155|a|520|520|1053579712|1053579724|1053580841|0|100664|0|113|155922|0
```

The output from `ils` is given in many columns, the meaning of which is explained in the `man` page. Of main interest in the search for deleted files, however, are the first, third and fourth columns. These show the file's inode number, user ID and group ID respectively. As for the rows of output, only the final row refers to a non-root user, so I ignored the

remainder. Therefore the inode number of 38155 should contain the data for the deleted file.

The Sleuth Kit's `icat` tool is ideal at this moment, as it provides for copying files by inode number. I used the following command to copy the contents of inode 38155 to a file in my `/tmp` directory:

```
[root@tortilla sleuthkit]# ./bin/icat -f linux-ext2 /dev/hda7 38155 > /tmp/junk1.rec
```

As the output from the temporary file shows, the `ils` and `icat` tools have successfully found the data being hidden via the method of unlinking an open file:

```
[root@tortilla sleuthkit]# cat /tmp/junk1.rec
user: tim          passwd: tim123
user: dawn         passwd: dawn123
user: david        passwd: david123
user: gareth       passwd: gareth123
```

Slack Space

In order to understand the use of slack space to hide data, one first has to understand a little about how computer hard disks are divided up and how operating systems read and write data to them. During a low-level format, hard disks are divided up into tracks and sectors so that operating systems can later use these divisions to store and find data. Tracks are concentric circles on a disk surface, whilst sectors are angular portions of the disk, like pieces of a pie. Most hard disks use a sector size of 512 bytes (Kuepper). After a high-level format has been performed, the filesystem will perform read and write operations on the disk in groupings of sectors called blocks (or clusters for the Windows operating system). On the ext2 file system a block will invariably be a grouping of either two, four or eight sectors - in other words 1024, 2048 or 4096 bytes (Chuvakin). The `/dev/hda7 (/home)` partition on my disk has a block size of 1024 bytes. Of course file sizes are only dependent on the amount of data being stored, and therefore are rarely exact multiples of block sizes. However, the effective space taken up by the file when written to the hard disk will always be a multiple of the block size. For example, a file of only ten bytes stored on a Linux partition that uses 1024 byte blocks will still take up 1024 bytes on the hard disk (1014 bytes will go unused). If exactly 1500 bytes of data is later appended to that file, giving it a file size of 1510 bytes, it will then take up 2048 bytes (ie two blocks) on the hard disk. The area on the hard disk between the end-of-file indicator and the final block boundary is referred to as the slack space for the file. As the slack space is not addressable by the file system, it can be used to hide data, although the amount of hidden data is limited to the file system's block size.

Hiding Data in Slack Space

There is a tool called `bmap` that can be used to access file slack space on Linux systems (superuser privileges are required). It was written by Daniel Ridge for Scyld Computing Corporation. I downloaded the RPM file `bmap-1.0.20-1.i386.rpm` from the following site:

ftp://ftp.scyld.com/pub/forensic_computing/bmap/RPMS/i386/

Before installing `bmap` yourself, please note that it may damage your hard disk. The README file states:

WARNING: This may spank your hard drive

I installed bmap with the following command:

```
[root@tortilla /]# rpm -iv bmap-1.0.20-1.i386.rpm
```

I created a directory of /home/sans/slack in which to experiment with bmap. I created two text files for the purpose of using them to hide data. The exact sizes of the files are shown by the following command:

```
[sans@tortilla slack]$ ls -l file?.txt
-rw-r--r-- 1 sans sans 10 May 21 15:54 file1.txt
-rw-r--r-- 1 sans sans 1503 May 21 15:54 file2.txt
```

As the /dev/hda7 (/home) partition on my disk has a block size of 1024 bytes, this is also the maximum size of file slack space I can use to hide data. For the purposes of this demonstration I used far less than that. The following commands show how I (after logging in as the superuser) hid the same text string, "cybercriminal", in both files using bmap with the putslack option:

```
[root@tortilla slack]# echo "cybercriminal" | bmap --putslack file1.txt
stuffing block 139522
file size was: 10
slack size: 1014
block size: 1024
```

```
[root@tortilla slack]# echo "cybercriminal" | bmap --putslack file2.txt
stuffing block 139524
file size was: 1503
slack size: 545
block size: 1024
```

The following commands demonstrate that the data has been hidden in the files' slack space. Firstly, I use bmap with the slack option to retrieve the contents of slack space for the two files. Secondly, I show that neither of the file sizes has changed; Linux is not aware of the hidden data. Thirdly, I confirm using grep and the cat command on the smaller file that the hidden data is not accessible via normal operating system utilities:

```
[root@tortilla slack]# bmap --slack file1.txt
getting from block 139522
file size was: 10
slack size: 1014
block size: 1024
cybercriminal
```

```
[root@tortilla slack]# bmap --slack file2.txt
getting from block 139524
file size was: 1503
slack size: 545
block size: 1024
cybercriminal
```

```
[root@tortilla slack]# ls -l file?.txt
-rw-r--r-- 1 sans sans 10 May 21 15:54 file1.txt
-rw-r--r-- 1 sans sans 1503 May 21 15:54 file2.txt
```

```
[root@tortilla slack]# grep cybercriminal *
```

```
[root@tortilla slack]# cat file1.txt
123456789
```

It should also be noted at this point that not even message digests produced with the `md5sum` utility will indicate the presence of data in the file slack space, as this utility operates only on the file contents.

The technique of hiding data in file slack space is seldom used because of two main reasons. Firstly, it does not allow for hiding large amounts of data. Even file systems with a block size of 4096 bytes are restricted to only 4KB of hidden data per file. Secondly, the technique is only useful for files that are very stable, as modifications to the file can make the hidden data inaccessible even to the tool responsible for its placement. As a demonstration, I used a text editor to delete the first character in the smaller of the two files containing hidden data. Subsequently I found that attempting to retrieve the hidden data with `bmap` (using the `slack` option) resulted in my screen filling with spurious characters. The tiniest modification to the file had caused my method of accessing its slack space to fail completely, although other slack space tools may be able to handle file modifications.

The limitations of this technique mean that it is very unlikely to be used by insiders as a method of hiding data. After all, legitimate users of the system presumably have the permissions to write and modify files, so they have plenty of opportunity to store small amounts of data. File slack space is more likely to be used by people who don't have the permission to write files on the system, such as hackers. For example, hackers could use the technique to store small Perl scripts or lists of cracked passwords.

Finding Data Hidden in Slack Space

Using Linux Utilities

The search for data hidden in file slack space is best done via a forensic investigation of the partition in question. To achieve this on my system, I first unmounted the `/home` partition and then used the `dd` utility to create an image of the partition to work with. The instructions for doing this are contained in the appendix "Creating a Forensic Image". I then used the `strings` utility to search the entire image. By default this command will output any strings of four or more printable characters that it finds within the given file (in this case the file is an image of the entire partition):

```
[root@tortilla /]# cd /usr/local/forensics

[root@tortilla forensics]# strings dev_hda7.img | grep "cybercriminal"
cybercriminal
cybercriminal
```

Although the search has been successful, it requires follow-up investigation on any matches because the output provided no information about where on the partition the strings were located. The lack of this information makes it difficult for investigators to see the strings in context, or even to establish that they were being stored in file slack space.

Using The Sleuth Kit / Autopsy

Autopsy provides the ability to search for key words in both allocated disk space and unallocated disk space. As file slack space falls into the category of allocated disk space (the relevant blocks have been allocated), this demonstration focuses on that portion of my `/dev/hda7` partition. The brief instructions for accomplishing this are:

- 1 Create an image of the partition as set out in the appendix "Creating a Forensic Image".
- 2 Assuming that a case and a host name have already been set up in previous sections, choose "Keyword Search" from the main menu. If this is the first time a search for a particular string is being conducted on the allocated portion of the forensic image, the "Extract Strings" button should be clicked. Autopsy will then go through the image and create an indexed file of all strings discovered. This file can be quite large - my 300 MB image resulted in a strings file of almost 40 MB – however, it enables upcoming searches to scan only the strings file rather than the entire image.
- 3 Enter the string to search for, in my case "cybercriminal", and click on the search button. The Autopsy output from my search identified two occurrences of this string. It also provided me with the block numbers on the partition where the strings were found, the offset within these blocks and links to view the blocks in either ASCII or hexadecimal. As shown in the following output, the block numbers (also referred to by Autopsy as Fragments or Data Units), were 139522 and 139524:

```
2 potential occurrences of cybercriminal were found
139522 (Hex - Ascii)
- offset 10 bytes
139524 (Hex - Ascii)
- offset 479 bytes
```

- 4 The Autopsy output is a significant improvement on the `strings` command I ran previously (admittedly the `strings` command was run without options). By providing the opportunity to view the block where the string was located, the string can be seen in context, which may provide vital clues in an investigation. I clicked on the "Ascii" link to see the contents of block 139522, although I could also have seen the block's contents by choosing "Data Unit" on the Autopsy main menu:

```
ASCII Contents of Fragment 139522 (1024 bytes) in images/dev_hda7.img
```

```
123456789
cybercriminal
```

- 5 Further information was provided when I clicked on the link to "ASCII report" - in particular, the name of the file that points to block 139522. An analysis of the file contents and the block contents may then lead an investigator to deduce that file slack space has been used to hide data:

```
Autopsy ascii Fragment Report (ver 1.71)
```

```
-----
Fragment: 139522
Length: 1024 bytes
Pointed to by Inode: 34138
Pointed to by files:
  /mnt/forensics/home/sans/slack/file1.txt
MD5 of raw Fragment: 377cef21391dd33d948afcdcc364b572
MD5 of ascii output: e64c7c4c4895b3bdcc672ca99208ff46
Image: /usr/local/forensics//sans/tortilla/images/dev_hda7.img
Image Type: linux-ext2
Date Generated: Fri May 23 13:42:34 2003
Investigator: gjr
-----
```


123456789
cybercriminal

© SANS Institute 2003, Author retains full rights.

Appendix

Creating a Forensic Image

Forensic examination of a suspect system should never be performed on the system itself. Instead, it should be performed on a trusted system, using images taken from the suspect disk. These images, which are exact bit-by-bit copies of the original partitions, effectively allow the system to be examined without fear of contaminating the original system state. Some of the techniques for finding hidden data that are discussed in this paper deal with a forensic image of the `/dev/hda7` partition on my system, mounted on the `/home` directory. Rather than duplicating the instructions for creating and mounting a forensic image in various places throughout the paper, I have outlined the necessary steps in this section, and the examples in the paper refer to them as required.

The `/dev/hda7` (`/home`) partition on my system is just over 300 MB in size, as shown by the following `df` command:

```
[root@tortilla root]# cd /

[root@tortilla /]# df -H
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda8        1.0GB   80MB  896MB   9% /
/dev/hda1         88MB   5.4MB   77MB   7% /boot
/dev/hda10        64MB    14kB   60MB   1% /hack
/dev/hda7        303MB   518kB  286MB   1% /home
none             97MB     0    97MB   0% /dev/shm
/dev/hda6        406MB   8.9MB  376MB   3% /tmp
/dev/hda2        5.0GB   1.8GB  2.9GB  38% /usr
/dev/hda3        2.3GB   58MB   2.1GB   3% /usr/local
/dev/hda5        406MB   35MB   350MB   9% /var
```

The output from the `df` command shows that I have enough room on any one of a number of other partitions to store an image of 300 MB for investigation. Although this violates one of the main rules for forensic investigation, it is okay for demonstration purposes. I now unmount the `/dev/hda7` device. This is necessary to stop any further file system interaction with the device, therefore preserving the data:

```
[root@tortilla /]# umount /dev/hda7
```

I now use the `dd` command to create a forensic image of my `/dev/hda7` (`/home`) partition. The image that results, `/usr/local/forensics/dev_hda7.img`, is an exact bit-by-bit copy of the partition. At various stages throughout this paper I create such an image for analysis with forensic tools:

```
[root@tortilla /]# dd if=/dev/hda7 of=/usr/local/forensics/dev_hda7.img
610406+0 records in
610406+0 records out
```

Note that upon completion of a section requiring the use of a forensic image, the subsequent section will require remounting of the partition (to effect the data hiding) and recreation of the image (to reflect the changes).

References

Bach, Maurice J. "The Design of the UNIX Operating System."
Prentice Hall. Englewood Cliffs, NJ. 1986.

Cheng, Derek. "Freeware Forensics Tools for UNIX." November 1 2001.
URL: <http://online.securityfocus.com/infocus/1503> (30 April 2003)

Chuvakin, Anton. "Linux Data Hiding and Recovery." 10 March 2002.
URL: http://www.linuxsecurity.com/feature_stories/data-hiding-forensics.html
(30 April 2003)

Crane, Aaron. "Linux Ext2fs Undeletion mini-HOWTO." Version 1.3. 2 February 1999.
URL: <http://www.tldp.org/HOWTO/mini/Ext2fs-Undeletion.html> (30 April 2003)

Di Pietro, Roberto and Mancini, Luigi V. "A Methodology for Computer Forensics Analysis."
Proceedings of the 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, New York. June 2002.

Dittrich, Dave. "Basic Steps in Forensic Analysis of UNIX Systems."
URL: <http://staff.washington.edu/dittrich/misc/forensics> (30 April 2003)

Farmer, Dan. "Bring Out Your Dead."
Dr Dobb's Journal. January 2001.
URL: <http://www.ddj.com/documents/s=871/ddj0101h/0101h.htm> (30 April 2003)

Green, John. "Basic Forensic Principles Illustrated with UNIX - Hands On."
Course Notes from SANS Conference, Sydney 2003, "Track 8 - System Forensics, Investigation and Response". SANS Institute. 2003.

Kruse, Warren G. II. and Heiser, Jay G. "Computer Forensics: Incident Response Essentials." Addison-Wesley. Boston, MA. 2001.

Kuepper, Brian. "What You Don't See On Your Hard Drive." 4 April 2002.
URL: <http://www.sans.org/rr/paper.php?id=653> (10 May 2003)

"Linux ext3 FAQ." Authors unknown. 9 April 2003.
URL: <http://batleth.sapienti-sat.org/projects/FAQs/ext3-faq.html> (15 May 2003)

Shinder, Debra L. "Scene of the Cybercrime."
Syngress Books. Rockland, MA. 2002.

Sorenson, Holt. "Incident Response Tools for Unix, Part One: System Tools."
27 March 2003.

URL: <http://www.securityfocus.com/infocus/1679> (30 April 2003)

Venema, Wietse. "File Recovery Techniques."

Dr Dobb's Journal. December 2000.

URL: <http://www.ddj.com/documents/s=878/ddj0012h/0012h.htm> (30 April 2003)

© SANS Institute 2003, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



| | | | |
|--|--|-----------------------------|------------|
| SANS Cyber Security West: Feb 2021 | , | Feb 01, 2021 - Feb 06, 2021 | CyberCon |
| Open-Source Intelligence Summit & Training 2021 | Virtual - US Eastern, | Feb 08, 2021 - Feb 23, 2021 | CyberCon |
| SANS Secure Japan 2021 | , Japan | Feb 22, 2021 - Mar 13, 2021 | CyberCon |
| SANS Scottsdale: Virtual Edition 2021 | , | Feb 22, 2021 - Feb 27, 2021 | CyberCon |
| SANS London February 2021 | Virtual - Greenwich Mean Time, United Kingdom | Feb 22, 2021 - Feb 27, 2021 | CyberCon |
| SANS Cyber Security East: March 2021 | , | Mar 01, 2021 - Mar 06, 2021 | CyberCon |
| SANS Secure Asia Pacific 2021 | Singapore, Singapore | Mar 08, 2021 - Mar 20, 2021 | Live Event |
| SANS Secure Asia Pacific 2021 | , Singapore | Mar 08, 2021 - Mar 20, 2021 | CyberCon |
| SANS Cyber Security West: March 2021 | , | Mar 15, 2021 - Mar 20, 2021 | CyberCon |
| SANS Riyadh March 2021 | , Kingdom Of Saudi Arabia | Mar 20, 2021 - Apr 01, 2021 | CyberCon |
| SANS Secure Australia 2021 | Canberra, Australia | Mar 22, 2021 - Mar 27, 2021 | Live Event |
| SANS Munich March 2021 | Virtual - Central European Time, Germany | Mar 22, 2021 - Mar 27, 2021 | CyberCon |
| SANS Secure Australia 2021 Live Online | , Australia | Mar 22, 2021 - Mar 27, 2021 | CyberCon |
| SANS 2021 | , | Mar 22, 2021 - Mar 27, 2021 | CyberCon |
| SANS Cyber Security Mountain: April 2021 | , | Apr 05, 2021 - Apr 10, 2021 | CyberCon |
| SANS SEC401 (In Spanish) April 2021 | Virtual - Central European Summer Time, Spain | Apr 12, 2021 - Apr 23, 2021 | CyberCon |
| SANS Cyber Security East: April 2021 | , | Apr 12, 2021 - Apr 17, 2021 | CyberCon |
| SANS London April 2021 | Virtual - British Summer Time, United Kingdom | Apr 12, 2021 - Apr 17, 2021 | CyberCon |
| SANS Autumn Australia 2021 | Sydney, Australia | Apr 12, 2021 - Apr 17, 2021 | Live Event |
| SANS Autumn Australia 2021 - Live Online | , Australia | Apr 12, 2021 - Apr 17, 2021 | CyberCon |
| SANS Secure India 2021 | , Singapore | Apr 19, 2021 - Apr 24, 2021 | CyberCon |
| SANS Baltimore Spring: Virtual Edition 2021 | , | Apr 26, 2021 - May 01, 2021 | CyberCon |
| SANS Cyber Security Central: May 2021 | , | May 03, 2021 - May 08, 2021 | CyberCon |
| SANS Security West 2021 | , | May 10, 2021 - May 15, 2021 | CyberCon |
| SANS Cyber Security East: May 2021 | , | May 17, 2021 - May 22, 2021 | CyberCon |
| SANS Stockholm May 2021 | Virtual - Central European Summer Time, Sweden | May 31, 2021 - Jun 05, 2021 | CyberCon |
| SANS In French May 2021 | Virtual - Central European Summer Time, France | May 31, 2021 - Jun 05, 2021 | CyberCon |
| SANS Cyber Security Central: June 2021 | , | Jun 07, 2021 - Jun 12, 2021 | CyberCon |
| SANS SOC Training 2021 | , | Jun 14, 2021 - Jun 19, 2021 | CyberCon |
| SANS Cyber Defence Asia Pacific 2021 - Live Online | , Australia | Jun 28, 2021 - Jul 10, 2021 | CyberCon |
| SANS Cyber Defence Asia Pacific 2021 | , Australia | Jun 28, 2021 - Jul 10, 2021 | Live Event |

The Biden Transition

Joe Biden may be the new president-elect — but with President Donald Trump continuing to challenge the results and Senate control up still up for grabs, the story of the election is far from over.

BIDEN'S PLANS

- Kathleen Hicks is **Biden's pick to be the first female deputy defense secretary.**
- Biden has tapped three senior officials onto **his Covid-19 Response team.**
- Biden's transition chief blasts 'obstruction' by political appointees **at OMB and the Pentagon.**
- Trump's unplanned gift to Biden is that **clean energy is on the rise.**

TRUMP AND THE GOP

- Sen. Josh Hawley **pledged to challenge Biden's victory in Pennsylvania** on Jan. 6.
- Nancy Pelosi will **seat a Republican in a contested Iowa race.**
- Congress and the coronavirus **could quash Trump's Electoral College gambit.**
- Sen. Ben Sasse delivered a critique of his Republican colleagues **challenging 2020 results.**

COMING UP: GEORGIA SENATE RUNOFFS

- A judge is seeking a **deal to limit voter challenges** in the Georgia runoff.
- Joe Biden and Kamala Harris **are going back to Georgia before the Senate runoffs.**
- Strong early voting turnout **gives Democrats hope in Georgia runoffs.**
- Sens. Kelly Loeffler and David Perdue **side with Trump on \$2,000 stimulus payments.**

FILED UNDER: TECHNOLOGY, INTELLECTUAL PROPERTY, BALLOT ACCESS, 2020 ELECTIONS, 2020 PRESIDENTIAL CANDIDATES

Help us do better!

To support and inform our journalism, it helps to learn more about you.

SENIORITY

Select Seniority

INDUSTRY

Select Industry

Submit

☐ STOP

The use of this information is governed by POLITICO's privacy policy and terms of service. You can contact us here. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

SPONSORED CONTENT

By |

Finally - A perfect mask to breathe freely

SportsMask.eu

1 In 2 Mac Users Are Unaware Of

MacKeeper

Could This Be The Largest Oil Find Of The

ReconAfrica

Shut The Front Door! The All New Subaru

Subaru | Sponsored Listings

Modern Japanese Method To Keep

Health Truth Finder

[Pics] Where Vice-president Kamala Harris

Hollywood Tale

Live Poll: Take the Official 2021 DNC

Paid for by the Democratic National Committee

All-Inclusive Cruise Packages Are

Luxury Travel | Sponsored Listings

The All New Subaru Outback Is Set To Amaze

Luxury Auto | Sponsored Listings

Here's What New Dental Implants

Dental Implants - Sponsored Listings

About Us

Advertising

Breaking News Alerts

Careers

Credit Card Payments

Digital Edition

FAQ

Feedback

Headlines

Photos

[POWERJobs](#)

[Press](#)

[Print Subscriptions](#)

[Write For Us](#)

[RSS](#)

[Site Map](#)

[Terms of Service](#)

[Privacy Policy](#)

[Do not sell my info](#)

[Notice to California Residents](#)

© 2021 POLITICO LLC